Chapter 2
United States of America

CONTENTS

1 INTRODUCTION

The United States does not have omnibus data protection legislation, protecting data privacy in the public and private sector alike. This does not mean that United States law offers no protection to "information privacy", the term American commentators prefer to the term "data protection". In fact, the "right to privacy" is widely considered an American concept in both origin and development.[1] Data protection, or data privacy or informational privacy, has its roots in the Federal Constitution and in common law, specifically tort law. However, the common law of privacy, and the more recent constitutional right to privacy, have proved to be of little help in the attempts to "fashion a public policy to deal with the dangers of information technology".[2] Because of the failure of judicial and constitutional interpretation to provide effective safeguards through case law against the new record-keeping practices that are the result of the increasing use of new computer technology, policy makers have had to turn to legislation. Data protection in the United States is thus principally achieved through a medley of different pieces of legislation.[3]

2 PROTECTION OF PRIVACY IN TORT LAW

2.1 Development of right to privacy in tort law

2.1.1 Right to be let alone

1 Bennett *Regulating privacy* 65.

2 Bennett *Regulating privacy* 67.

3 One should also keep in mind that the USA is a member of the OECD and several hundred US companies have adopted the OECD Guidelines on data protection (see ch 3 par 2.1). In the private sector one therefore finds that fair information practices have been created through industry self-regulation. The application of these principles is voluntary and they are not legally binding on the companies. As such they may be changed at any time by the companies involved. See Schwartz & Reidenberg *Data privacy law* 11. Also see GILC *Privacy and human rights* 23–24.

Before 1890 no English or American court recognised a right to privacy.[4] At the end of that year Warren and Brandeis published their now famous law review article "The Right to Privacy",[5] in which they contended that common law implicitly recognised the right to privacy. Their article "enjoys the unique distinction of having initiated and theoretically outlined a new field of jurisprudence".[6]

They argued[7] that the courts had in the past granted relief for the invasion of privacy on a combination of different common law doctrines[8] but that in essence the courts were protecting the individual's "right to be let alone"[9] as part of the more general right to one's personality.[10] They contended that new inventions and business methods made the recognition of the right to privacy necessary.[11] They declared that "the intensity and complexity of life, attendant upon advances in civilization" and "modern enterprise and invention" subject the individual to mental pain and stress, far greater than could be inflicted by mere bodily injury.[12]

---

4 Keeton *Law of torts* 849; Trubow *Invited papers* 2.

5 Warren & Brandeis 1890 *Harv LR* 193.

6 Larremore 1912 *Colum LR* 693; Turkington & Allen *Privacy law* 38. Also see McQuoid-Mason *Privacy* 35; Neethling *Privaatheid* 152; *National Media v Jooste* 1996 3 SA 262 (A) 267–268.

7 Warren & Brandeis 1890 *Harv LR* 193, 207–212.

8 Eg on the basis of defamation, a property right (eg *Prince Albert v Strange* (1849) ER 1171 where private letters were published), breach of confidence or an implied contract (eg *Yovatt v Winyard* (1820) 37 Eng Rep 425 where recipes that had been obtained surreptitiously by an employee were published).

9 Warren & Brandeis 1890 *Harv LR* 193, 195. See also ch 1 par 1.5.

10 Warren & Brandeis 1890 *Harv LR* 193, 205, 207.

11 Warren & Brandeis 1890 *Harv LR* 193–195:

> Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society... Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual... the right 'to be let alone.' Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the incision of privacy by the newspapers, long keenly felt, has been but recently discussed...

12 Warren & Brandeis 1890 *Harv LR* 193, 196.

Warren and Brandeis' main concern was that information about one's personal life should not be revealed to the public by the press.[13] They consequently limit the right to privacy by allowing the publication of material that is of public or general concern,[14] by granting the same privileges of publication as apply in defamation,[15] and by excluding oral publications in the absence of special damages.[16] The right to privacy would also cease upon the publication of the facts by the individual concerned or with his or her consent.[17] The truth of the published matter and the absence of malice afford no defence, however.[18] The remedies for an invasion of the right to privacy are the same as in the law of defamation and "artistic property", namely a tort action for damages, and an injunction in a limited number of cases.[19]

Subsequent authors have pursued the same theme, and according to Keeton no other tort has received such an outpouring of comment in advocacy of its bare existence.[20] However, the precise right they advocated – a privacy right for the publication of private facts – has not fared well.[21] During the last century four tort privacy rights have come into being, each with its own set of requirements, limiting the

13 Warren and Brandeis wrote the article after a spate of gossip appeared in the Boston newspapers about the social affairs of Mrs Warren, the daughter of a senator from Delaware and one of Boston's élite. Boston was one of the cities "where a lady and a gentleman kept their names and their personal affairs out of the papers" (Prosser 1960 *Cal L R* 383) and when the press had a field day with the wedding of their daughter, Warren became annoyed. Prosser 423 surmises that "she must have been a very beautiful girl", because "[t]his was the face that launched a thousand lawsuits".

14 Warren & Brandeis 1890 *Harv LR* 193, 214.

15 I e, publications "made in a court of justice... or any body quasipublic", or "made by one in the discharge of some public or private duty" (Warren & Brandeis 1890 *Harv LR* 193, 216–217).

16 Warren & Brandeis 1890 *Harv LR* 193, 217.

17 Warren & Brandeis 1890 *Harv LR* 193, 218.

18 Warren & Brandeis 1890 *Harv LR* 193, 218.

19 Warren & Brandeis 1890 *Harv LR* 193, 219.

20 See Keeton *Law of torts* 850 and authors cited by him in fn 9.

21 Turkington 1997 *JL Med & Ethics* 113, 119.

usefulness of these torts for the protection of the privacy of personal information.[22]

2.1.2 Prosser's four distinct torts

The courts and legislatures[23] began to apply the Warren-Brandeis' "right to privacy" terminology to situations other than the publication of information about individuals.[24] In 1960 Prosser concluded that the overwhelming majority of American courts had declared that privacy in one form or another existed.[25] Prosser was of the opinion, however, that what emerged from those decisions was not one tort, but a complex of four, which are tied together by the common name "right to privacy" but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff "to be let alone".[26]

He described these four torts as follows:[27]

- intrusion upon the plaintiff's seclusion or solitude, or into his or her private affairs
- public disclosure of embarrassing private facts about the plaintiff

22 Turkington 1997 *JL Med & Ethics* 113, 119.

23 The first state to enact privacy legislation was New York in 1903 (NY Sess Laws 1903 ch 132 ss 1–2). In this legislation it was made a misdemeanour to make use of the name, portrait or picture of any person for advertising purposes or for purposes of trade without that person's written consent. The legislature enacted the statute in reaction to a decision by the New York Court of Appeals (*Roberson v Rochester Folding-Box Co* 171 NY 538, 64 NE 442 (1902)). In this case the court denied that the plaintiff, a young woman whose picture was used by the defendant to advertise its flour without her consent, had any right of protection. Before the *Roberson* decision, the NY lower courts had accepted the existence of the right to privacy (Keeton *Law of torts* 850 fn 10).

A few years later the Georgia Supreme Court (*Pavesich v New England Life Insurance Co* 122 Ga 190, 50 SE 68 (1905)) had no trouble in accepting the view of Warren and Brandeis, and recognised the existence of a right to privacy in a case where the facts were similar to those of the *Roberson* case. *Pavesich* became the leading case, and in 1938 the first Restatement of Torts s 867 recognised a cause of action against any one who "unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public" (see Elder *Law of privacy* 2–3). See further Turkington & Allen *Privacy law* 52–58; McQuoid-Mason *Privacy* 36–37.

24 Prosser 1960 *Cal LR* 383, 385–388.

25 Prosser 1960 *Cal LR* 383, 386. By 1980 Rhode Island was the only state not recognising a right to privacy in some form (Keeton *Law of torts* 851).

26 Prosser 1960 *Cal LR* 383, 389.

27 Prosser 1960 *Cal LR* 383, 389.

- ❒ publicity that places the plaintiff in a false light in the public eye
- ❒ appropriation, for the defendant's advantage, of the plaintiff's name or likeness

Prosser's framework of four torts became widely accepted, despite criticism,[28] and in 1977 the *Restatement (Second) of Torts*[29] accepted this division.[30]

2.1.2.1 Intrusion tort

The intrusion tort[31] is the intentional interference with another's interest in solitude or seclusion, and has been applied in cases of physical intrusions, eavesdropping, surveillance and inspection of privately held records.[32] Three requirements must be satisfied:[33]

- ❒ There must be something in the nature of prying or intrusion (disturbing noises and bad manners do not suffice).
- ❒ The intrusion must offend a reasonable person.
- ❒ It must be an intrusion into something that is, and is entitled to be, private.

2.1.2.2 Public disclosure tort / private facts tort

28 Bloustein 1964 *NYULR* 962 criticised Prosser's division of privacy into four separate torts. He argued that it undermined the Warren and Brandeis axiom of "inviolate personality" and neglected its moral basis as an aspect of human dignity.

29 *Restatement (Second) of Torts* s 652B (s 625E (1977)).

30 Also see ch 7 par 2.3.2.1 for a discussion of the issue whether these torts protect privacy, or perhaps some other aspect of personality.

31 Restatement (Second) of Torts s 652B provides:

> Intrusion upon seclusion. One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

32 Keeton *Law of torts* 854.

33 Keeton *Law of torts* 855; Wacks*Privacy (vol II)* xii. For an extensive discussion of this tort, see Elder *Law of privacy*15–147. Also see McQuoid-Mason *Privacy* 37–38 and Neethling *Privaatheid* 167–183.

The second of these torts, the private facts tort,[34] was the one Warren and Brandeis had in mind in their article. This tort invades the individual's interest in his or her reputation, and has the same overtones of mental distress that are present in libel and slander. However, it differs from libel and slander in that truth is not a defence[35] and no wrongful motive is required.[36] Prosser indicates the following requirements:[37]

- There must be publicity.
- The facts disclosed must be private.
- The facts disclosed must be offensive and objectionable to a reasonable person of ordinary sensibilities.

To this the Restatement adds the requirement that the matter published should be published to the public at large and should not be of legitimate concern to the public.[38] Thus, publication of the facts contained in a public record or left open to the public eye by the individual concerned does not invade such an individual's privacy.[39]

2.1.2.3 False light tort

34 Restatement (Second) of Torts s 652D provides:

> Publicity given to private life. One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
> (a) would be highly offensive to a reasonable person, and
> (b) is not of legitimate concern to the public.

35 Prosser 1960 *Cal LR* 383, 422; McQuoid-Mason *Privacy* 37–38. This tort is "an extension of defamation into the field of publications that do not fall within the narrow limits of the common law defamation tort" (Elder *Law of privacy* 150).

36 Malice is required, however, as a precondition for the award of punitive damages, and to determine whether the defendant has forfeited a privileged occasion (Elder *Law of privacy* 150–151).

37 Prosser 1960 *Cal LR* 383, 393–396.

38 Restatement (Second) of Torts s 652D.

39 See further Elder *Law of privacy* 149–260. Also see McQuoid-Mason *Privacy* 38–39 and Neethling *Privaatheid* 183–191.

The false-light tort[40] consists of publicity that places a person in a false light in the public eye.[41] An action based on this tort can overlap with an action for defamation, but whereas an action for defamation concerns the protection of a person's reputation, the false light tort is an invasion of a person's right to be left alone.[42] The requirements for this tort are:[43]

- Publication to the public at large.
- The publication should be of such a nature that a reasonable person would consider it highly offensive.
- The matter published should be false.

2.1.2.4 Appropriation tort

The appropriation tort[44] involves the tortuous use of a person's identity by a defendant for some advantage of his or her own, for example, impersonation to obtain credit or secret information.[45]

2.2 Utility of privacy torts in protecting information or data privacy

40 Restatement (Second) of Torts s 652E provides:

> Publicity placing person in false light. One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if
> (a) the false light in which the other was placed would be highly offensive to a reasonable person, and
> (b) the actor had knowledge or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

41 Eg, the unauthorised use of a plaintiff's name, or attributing to the plaintiff some opinion or utterance (Keeton *Law of torts* 863).

42 Keeton *Law of torts* 865. The plaintiff is entitled to obtain only a single recovery for dual claims arising out of the same facts (Elder *Law of privacy* 261).

43 Keeton *Law of torts* 863–865. See further McQuoid-Mason *Privacy* 40 and Neethling *Privaatheid* 191–196.

44 Restatement (Second) of Torts s 652C provides:

> Appropriation of name or likeness. One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.

45 Keeton *Law of torts* 852; McQuoid-Mason *Privacy* 40–43 and Neethling *Privaatheid* 196–202. This was the first form of privacy invasion to be recognised by the courts and legislature (see fn 23) and has established what is called "a right of publicity" under which individuals are able to decide how they wish to exploit their names commercially (see Wacks *Privacy (vol II)* xiii; Trubow 1985 *J Mar LR* 815, 819).

As the constitutional right to privacy only protects individuals when the government infringes upon their right to privacy,[46] and as legislation to protect the privacy of personal information in the private sector is limited to specific areas,[47] a litigant may sometimes only have a tort privacy right to rely on. Unfortunately the tort privacy rights can at best provide limited protection to information privacy.[48]

The intrusion tort could be invoked in cases such as intentional and unauthorised accessing of private records.[49] However, to qualify for this protection, the intrusion must satisfy a high threshold of "offensiveness"[50] and there must be something in the nature of prying or intrusion.[51] Voluntarily disclosed personal information would fall outside the scope of this right.[52] One commentator argues that this tort may be invoked as a protection against electronic violations in those areas in which there is a legitimate expectation of privacy.[53]

The private facts or public disclosure tort may play a role when private facts are published to the public

46 See Schwartz 1989 *Am J Comp L* 675, 679 and see further par 3.

47 See par 4.1.

48 See in general Reidenberg 1995 *Iowa LR* 497, 504–505; Reidenberg 1992 *Fed Comm LJ* 195, 221–226.

49 See Turkington 1997 *JL Med & Ethics* 113, 119.

50 Schwartz & Reidenberg *Data privacy law* 328–329. According to these authors, the surreptitious collection of personal information without notice or consent is not likely to be sufficiently objectionable.

51 Schwartz & Reidenberg *Data privacy law* 181. These authors illustrate the inadequacy of the intrusion tort for protecting medical privacy with reference to *Miller v Motorola* 560 NE 2d 900 (Ill App Ct 1990). In this case an employer disclosed sensitive medical information to the plaintiff's co-workers. The Illinois court found the plaintiff to have suffered no intrusion because she had voluntarily provided the information to her employer. Cate *Information age* 89 is of the opinion that this tort lends little support to information privacy, other than as a potential restriction on the means of gathering information.

52 Reidenberg 1992 *Fed Comm LJ* 195, 223. Reidenberg also points out that this privacy right is only relevant when information is collected. It does not address other data protection practices such as the storage, use and disclosure of personal information.

53 See Campbell *Data transmission and privacy* 501. Campbell gives examples of computer related intrusions, some of which are:
- unauthorised access to an individual's database contained on the individual's or another's computer
- unauthorised aggregation of data on an individual's associations, habits, movements, and lifestyle
- unauthorised interception of e-mail or other data transmissions

at large. Again, however, "any claim would be difficult to sustain because the disclosure must meet a standard of being highly offensive to a reasonable person".[54] Courts have furthermore ruled that the restricted distribution of personal information to small groups of recipients does not qualify as a public disclosure.[55] Another aspect that restricts the public disclosure tort is that it has usually been held to require disclosure to someone without a legitimate interest in the information.[56] Also, personal information voluntarily disclosed or available from public sources is not protected.[57]

The false light tort and the appropriation tort are even less likely to be useful in protecting the privacy of personal information.[58] According to Wacks the appropriation tort essentially protects a proprietary interest and he finds it difficult to see how it is connected with the protection of privacy.[59] Reidenberg argues that when the personal information being processed approaches a profile of an individual, it is possible to view commercial uses as an appropriation of the individual's personality.[60]

The false light tort requires that the information published must be false and since the publication of

54 Schwartz & Reidenberg *Data privacy law* 334. In *Tacoma Public Library v Wossner* 951 P 2d 357 (Wash Ct App 1998) a Washington state court held that the disclosure of public employees' social security numbers "would be highly offensive to a reasonable person and not of legitimate concern to the public". However, the court allowed the disclosure of names, salaries and benefit information. See further Komuves 1998 *J Mar J Computer & Inf L* 529, 565.

55 Schwartz & Reidenberg *Data privacy law* 181 334. According to these authors, not even marketing lists identifying impotent men or buyers of skimpy underwear are likely to give rise to any tort cause of action. While these lists are offensive to reasonable persons, they are not likely to circulate to a sufficiently wide audience to qualify as a public disclosure. However, no case has been brought as yet in the direct marketing field to test their viewpoint.

56 Schwartz & Reidenberg *Data privacy law* 181.

57 Reidenberg 1992 *Fed Comm LJ* 195, 223–224. As a result, Reidenberg points out, activities such as the preparation and dissemination of intimate personal profiles from disparate public sources of information or the public revelation of information would not be actionable.

58 Wacks *Privacy (vol II)* xiii argues that the torts of "intrusion" and "public disclosure" are the only privacy torts that require the invasion of "something secret, secluded or private pertaining to the plaintiff", and that the torts of "appropriation" and "false light" "are not properly conceived of as aspects of privacy". Also see Zimmerman 1989 *NYULR* 364; Gross 1967 *NYULR* 34, 36 and Neethling *Privaatheid* 163–165.

59 Wacks *Privacy (vol II)* xiii. Also see Langan 1979 *Colum JL & Soc Probs* 143, 154–155.

60 Reidenberg 1992 *Fed Comm LJ* 195, 226.

private information implies the publication of information that is true, this tort has limited application.[61]

Although the public disclosure tort might seem to be the most useful in the protection of the privacy of personal information, the requirement that the private information should be published to the public at large brings this tort into conflict with freedom of speech as guaranteed by the First and Fourteenth Amendments of the US Constitution.[62] According to one commentator, this tort "has been

61 It was stated previously (see text to fn 43) that it may be used where a person was impersonated to obtain credit or secret information about that person. (But see ch 7 par 2.3.2.1.)

62 US Const Amendment I provides *inter alia*: "Congress shall make no law ... abridging the freedom of speech, or of the press... ." Even though the First Amendment does not explicitly refer to the states, they are bound by its provisions (as they are bound by the other amendments) by virtue of the Fourteenth Amendment's due process clause, which is interpreted as incorporating most of the Bill of Rights' guarantees. US Const Amendment XIV provides: "No state shall ... deprive any person of life, liberty, or property, without due process of law ... ."

The constitutionality of the private facts or public disclosure tort, involving the publication of truthful information, is especially suspect whenever the publication complained about is a publication by the press of truthful information that is of public interest. This conclusion can be drawn from a reading of the cases decided by the Supreme Court in this area. Four cases that involve speech that the plaintiff claimed to have been invasive of privacy have reached the Supreme Court, and in all four cases the court denied recovery: *Cox Broadcasting Corp v Cohn* 420 US 469 (1975);*Oklahoma Publishing Co v District Court* 430 US 308 (1977); *Smith v Daily Mail Publishing Co* 443 US 97 (1979); *Florida Star v BJF* 109 S Ct 2603 (1989). *Oklahoma* and *Smith* both involved the publication of the name of a juvenile murderer. In both cases the court unanimously held that the publication cannot be prohibited because the information was either obtained at court proceedings which were open to the public (*Oklahoma*) or was lawfully obtained from witnesses (*Smith*) and was a matter of public significance. *Cox* and *Florida Star* both involved the publication of a rape victim's name. In *Cox* the name of the victim was mentioned on the air by a television reporter, who got the name from the indictments of those charged with the rape. The court held that "interests in privacy fade when the information involved already appears on the public record" (494–495). In the *Florida Star* case, the rape victim's name was not made part of the public record – in fact Florida law required that rape victims' names should be kept confidential. The sheriff's department inadvertently disclosed the name in the incident report, which they placed in their press room. However, the press room had a sign stating that it was against the law to publish the name of a rape victim. A trainee reporter copied the name from the incident report and this was later published in the Florida Star newspaper. The majority of the Supreme Court held that the information was lawfully obtained and relied on the holding in *Cox* that if the media has lawfully obtained truthful information about a matter of public significance, then publication may not constitutionally be subject to sanctions in the absence of a need to further a state interest of the highest order. White J, who gave judgment for the majority in *Cox*, dissented in *Florida Star*. He was of the opinion that the result of the majority decision was to "obliterate one of the most noteworthy legal inventions of the 20th century: the tort of the publication of private facts" (2618). (Compare the above decisions with *US Dept of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989) – see par 3.2.2 below.) For a critical discussion of the *Florida Star* case, see Edelman 1990 *Tex LR* 1195 and Stanton 1991 *Hastings Con LQ* 391.

Some commentators are of the opinion that for an information privacy tort to succeed, the Supreme Court would have to decide that the publication of truthful information can in certain circumstances be sanctioned (see eg Trubow *Invited papers* 1). Other commentators are more positive and argue that the information privacy tort is not unconstitutional. In this regard, it has been argued that dissemination of

(continued...)

overwhelmed by the court's view that the free speech right trumps the privacy right".[63]

In conclusion it seems that Prosser's and the Restatement's division of the privacy tort into four categories or four separate torts have stultified any further development of the privacy tort that could have allowed for coverage of an invasion of privacy by the misuse of data.[64] Although the privacy torts have been "virtually irrelevant" in dealing with data protection issues in the USA,[65] the fact that a right

62(...continued)
personal information by private entities for profit is, like commercial speech, not protected by the First Amendment (Graham 1987 *Tex LR* 1395, 1436). Also see Volokh 2000 *Stanford LR* 1049 and Schwartz 2000 *Stanford LR* 1559.

63 Turkington 1997 *JL Med & Ethics* 113, 119. According to Cate *Information age* 90 only one award to a privacy tort plaintiff has ever survived the Supreme Court's First Amendment scrutiny, ie in *Cantrell v Forest City Plumbing Co* 419 US 245 (1974).

64 Graham 1987 *Tex LR* 1395, 1419 suggests two possible ways in which the common law of torts could still be used to protect privacy against invasions by the use of computers: One possibility is for courts to recognise privacy as a unified concept, and to protect information privacy by "stretching" one of the four existing categories (1427–1428):

> Although the courts so far have rejected the argument, the appropriation tort could be stretched to cover the situation in which an individual profile, instead of a name or likeness, is used by another. Of course the profile is not used to advertise in the traditional sense, but it is used to enhance marketing efforts and thus might be considered effectively equivalent... The intrusion tort may also cover the commercial dissemination of private facts... The intrusion torts at times had been applied in an "extended sense to protect personal information about an individual" [Tapper *Computer Law* 144 (1978)]. The transfer of personal information may itself be considered a cognizable intrusion because the intrusion that was permitted was only for a limited purpose – that for which the individual originally gave the information. Thus, the subsequent transfer violates the original understanding of the person giving the information. The private facts tort may also be more malleable than it would initially appear. The stumbling block here is the requirement of 'unreasonable publicity". ... Because computers easily transfer information, it is possible for so many persons to gain access to the information that it becomes public – at least enough to fall within the private facts tort.

Another possibility, and one which Graham favours, is the recognition of a new tort described as "tortuous commercial dissemination of private facts" (1428). Blackman 1993 *Santa Clara Computer & High Tech LJ* 431, 448, however, argues that a better common law basis than tort law for protecting "informational privacy" would be either the law of contract or the law of property. In order to use the law of property as a basis, however, information would first have to be defined as property (448). Using contract law is also problematic because it is difficult to show "actual damages" in cases involving eg "data profiling" (452). In the end Blackman concludes that legislation (particularly in the private sector) is needed to protect "informational privacy" (452):

> Although the common law provides the theoretical support, at least in the tort and contract realms, for finding informational privacy rights, the courts can not usurp the legislature's responsibility to write the law necessary to protect informational privacy.

65 See Bennett *Regulating privacy* 67.

to privacy is recognised by tort law[66] is very important for data protection purposes. This recognition has made it possible for Congress to pass legislation that protects privacy interests against threatened invasions that are a result of the new technology with which the common law tort principles have been unable to cope.

3 PROTECTION OF DATA PRIVACY UNDER FEDERAL CONSTITUTION

3.1 Introduction

As a point of departure, two characteristics of American constitutional law should be kept in mind: In the first place, constitutional rights are usually not applicable unless "state action" can be found.[67] This means that the rights created by the Constitution protect the individual from the government and not from private entities.[68] Secondly, the rights created by the Constitution are "negative rights" – they prevent certain kinds of governmental action, but place no affirmative duties on the state to protect the constitutional rights of individuals by actions such as the adoption of legislation.[69]

3.2 Development of constitutional right to privacy

The United States Constitution does not contain an explicit clause protecting the individual's right to

66 And more recently also under the Constitution.

67 The Thirteenth Amendment, which forbade slavery and involuntary servitude, is an exception to this rule.

68 A private entity's processing of personal data would therefore not be subject to a constitutional right to information privacy (see Schwartz & Reidenberg *Data privacy law* 33). Note, however, that state action can be found where a private entity takes over a public function in which the government is usually engaged, or when sufficient mutual contacts have occurred between the private entity and the government (see cases cited by Schwartz & Reidenberg *Data privacy law* 33 fn 7). Also see Cate *Information age* 50–51.

69 Schwartz & Reidenberg *Data privacy law* 32. This means that there is no duty on the government to actively protect an individual against invasion of his or her informational privacy rights. Rights of this kind are referred to as *Abwehrrechte* in German law (see Schwartz 1989 *Am J Comp L* 675, 679). Also see Cate *Information age* 51.

privacy.[70] A constitutionally based privacy right was developed by the Supreme Court from explicit constitutional protections against search and seizure, probable cause and self incrimination, as contained in the Third,[71] Fourth,[72] and Fifth[73] Amendments.[74] This development has been slow and irregular.[75] A distinction can be drawn between two types of privacy rights that have developed: substantive privacy rights and informational privacy rights.[76]

---

70 Unlike the Federal Constitution, the constitutions of some of the individual states do specifically recognise the right to privacy. See eg the Constitutions of Florida (Fla Const art 1 s 23), Illinois (Ill Const art I s 6), Louisiana (La Const art I s 5), South-Carolina (SC Const art I s 10); Alaska (Alaska Const art I s 22), Hawaii (Hawaii Const art 1 s 6), Montana (Mont Const art II s 10), California (Cal Const art I s 1), and Washington (Wash Const art I s 7).

Because there has been little judicial interpretation, it is difficult to draw a conclusion on how effective the privacy clauses of the state Constitutions are. Since most of them are more explicit in their language than the Federal Constitution, they arguably do grant state citizens more data privacy than the Federal Constitution does.

71 US Const Amend III provides:

> No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

72 US Const Amend IV, provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation and particularly describing the place to be searched, and the persons or things to be seized.

73 US Const Amend V, provides:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

74 Initially these amendments were interpreted as protecting only physical privacy (see eg *Olmstead v US* 277 US 438 (1928)), but they were later interpreted as protecting "people, not places", so that wiretapping of a public booth was eg held to violate the Fourth Amendment (see *Katz v US* 389 US 347 (1967)).

75 On the development of the constitutional right to privacy, see Tribe *Constitutional law* 1302 *et seq*; Leigh 1976 *Hastings Con LQ* 229; Langan 1979 *Colum JL & Soc Probs* 143; Hosch 1983 *Vand LR* 139, 151; Peck 1984 *Hofstra LR* 893; Seng 1985 *J Mar LR* 871; Heaney 1986 *Fordham Urb LJ* 927; Rubenfeld 1989 *Harv LR* 737; Freedman *Computer age* 75–85; Hixon *Public society* 71–89; Rubin *Private rights* 25–27; Maxwell & Reinsch "Freedom of Information Act" 84–85.

76 See Rubenfeld 1989 *Harv LR* 737, 740, 749; Komuves 1998 *J Mar J Computer & Inf L* 529, 561; Du Plessis & De Ville *Personal rights* 244; Devenish *SA Bill of Rights* 139–144.

3.2.1 Substantive privacy rights

A constitutional right of privacy involving "fundamental decision-making"[77] and also referred to as substantive privacy rights, was developed by the Supreme Court; this right first came into question in *Griswold v Connecticut*.[78] Douglas J, writing for the majority, asserted that a right to privacy exists which predates the Bill of Rights, and that several of the Bill of Rights' guarantees protect privacy interests by creating a "penumbra" or "zone of privacy".[79] In *Roe v Wade*[80] it was held that this right to privacy is part of the "liberty" protected by the Fifth and the Fourteenth Amendments, and that it is therefore a substantive due process right.[81] Although these cases recognised that a right to privacy is implicit in the Constitution, they did not delineate the scope of such right. However, in *Griswold* and subsequent cases,[82] decisions in matters of childbearing, such as the use of contraceptives or abortions,

77 Cate *Information age* 60.

78 381 US 479 (1965). Also see Maditisi 1992 *De Rebus* 659 *et seq*.

79 Douglas J held (*Griswold v Connecticut* 381 US 479 (1965)) at 484:

> Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one... The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment [is another]. The Fifth Amendment in its self-incrimination clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."...

Other members of the majority wrote separate opinions offering different privacy right sources. Justice Goldberg located the right in the Ninth Amendment, whereas Justices Harlan and White found it in the due process clause of the Fourteenth Amendment. See further Falby 1982 *Geo LJ* 219, 225 fn 51.

80 *Roe v Wade* 410 US 113 (1973).

81 *Roe v Wade* 410 US 113 (1973) 153.

The Supreme Court has interpreted the due process clause as providing two different types of constitutional protection:

(a) the government cannot deprive an individual of liberty without adequate procedural safeguards (the doctrine of procedural due process);
(b) even though there are procedural safeguards there are limits on the government's ability to take away liberty (the doctrine of substantive due process).

The substantive due process doctrine provides that the deprivation of liberty must bear a "reasonable relation" to a state purpose. However, whenever the state intrusion impacts on certain liberties, a stricter test than "reasonable relation" is used. Privacy is one of these liberties where a heightened scrutiny test is applied. See further Tribe *Constitutional law* 501–502 and Falby 1982 *Geo LJ* 219 225 fn 53.

82 See *Eisenstadt v Baird* 405 US 438 (1972);*Carey v Population Services Int'l* 431 US 678 (1977);*Roe v Wade* (continued...)

were considered part of the protected zone of privacy.[83]

3.2.2 Informational privacy rights

Informational privacy rights refer to the right to govern the conduct of others who intrude in various ways upon one's life; privacy in this sense limits the ability of others to gain, disseminate, or use information about oneself.[84] Constitutional informational privacy rights were developed around the Fourth Amendment's prohibition against unreasonable searches and seizures[85] and the Fourteenth Amendment's due process requirement.[86]

The Fourth Amendment was relied on in those cases where the issue was an intrusion upon a person's private information, for example through the use of an electronic listening device.[87] However, the Fourth Amendment proved to be of limited value for purposes of protecting informational privacy interests outside the criminal defence context.[88] Schwartz[89] explains why this is so:

> When deciding whether governmental conduct impinges upon a Fourth Amendment privacy interest, the Supreme Court evaluates the expectations of the individual and of society. A search is subject to the safeguards of the Fourth Amendment only if the object of the search has an actual, subjective expectation of privacy and society is

82(...continued)
410 US 113.

83 As a matter of fact, the right of autonomy or self determination is a better description than "privacy" of the nature of the rights the US Supreme Court considered to be worthy of constitutional protection in these cases. For criticism of this interpretation of privacy, see Neethling *Privaatheid* 303; *Persoonlikheidsreg* 43. Also see ch 7 par 2.3.2.1.

84 See Rubenfeld 1989 *Harv LR* 737 740.

85 See fn 72.

86 See fn 62.

87 See *Katz v US* 389 US 347 (1967) and fn 74.

88 Cate *Information age* 58 *et seq*.

89 Schwartz 1989 *Am J Comp L* 675, 680.

prepared to recognize this expectation as reasonable.[90]

Schwartz refers to two "glosses" on the Supreme Court's testing of expectations that impose a limitation on the usefulness of the Fourth Amendment privacy right when the government processes personal information:[91]

- A reasonable expectation of privacy attaches neither to activities that take place in "public" nor to objects controlled by third parties. If the state can see the activity, either through the agency of one of its officials or by means of enhanced technology, or can find evidence of it elsewhere, the Fourth Amendment offers no protection to the individual. As governmental data use involves data activities that take place outside the control of the individual, the Fourth Amendment has little value when the government has personal information in its computers.[92]

- Reasonable expectations of privacy attach only to activities that the individual treats as secret. Knowledge of the activity or of the information must therefore be extremely limited if there is to be any protection by the Fourth Amendment. However, personal information obtained by the government cannot be expected to remain secret in this sense – in fact, it will sometimes not even be treated as especially confidential.

In *US v Miller*[93] the Supreme Court denied that an individual has a Fourth Amendment expectation of privacy with respect to cheques and deposit slips that he or she voluntarily conveys to a bank and thereby exposes to its employees in the ordinary course of business. The court held that the depositor "takes the risk in revealing his affairs to another, that the information will be conveyed by that person

90 *Oliver v US* 466 US 170, 177–181 (1984); *Smith v Maryland* 442 US 735, 740–741 (1979); *US v White* 401 US 745 (1975); *Katz v US* 389 US 347, 361–62 (1967). Also see ch 8 par 3.1.2.

91 Schwartz 1989 *Am J Comp L* 675, 680–681.

92 Also see Schwartz 1995 *Iowa LR* 553, 572.

93 425 US 435 (1976).

to the government".[94] And in *Smith v Maryland*[95] it was held that individuals have no legitimate expectation of privacy regarding the telephone numbers that they dialled, because these numbers are routinely recorded by the telephone company for billing purposes.[96]

The Fourth Amendment's "reasonable expectation of privacy" approach makes it unsuitable for protecting privacy in the information age. In *Whalen v Roe*,[97] a case dealing not with intrusion but with disclosure of information, the Supreme Court therefore had recourse to the Fourteenth Amendment for the recognition of a "non-disclosure" privacy right.[98]

In *Whalen* the plaintiffs challenged the constitutionality of a New York statute that required the disclosure and recording in a computer bank of the names of users of certain prescription drugs. The names of the drug users, together with other relevant information, were stored in a data bank for five years. Strict nondisclosure regulations were imposed. Plaintiffs contended that there were two infringements upon their constitutional rights. Firstly, inadvertent or deliberate disclosure of their drug use by the government could seriously affect their reputation, and secondly, this threat to their reputation could impair their decision-making capacity about their health care.

---

94 *US v Miller* 425 US 435 (1976) 443. Justices Brennan and Marshall dissented. Congress also disagreed with this decision, and enacted the Right to Financial Privacy Act of 1978, which requires that bank customers must be served with a copy of any federal subpoena or summons in court, prior to its execution. See further fn 127.

95 442 US 735 (1979). Stewart J dissented.

96 Tribe *Constitutional law* 1391 argues that the "assumption of risk" or "assumption of broadcast" notion that underlies the holdings in *Smith v Maryland* 442 US 735 (1979) and *US v Miller* 425 US 435 (1976)

> reveals alarming tendencies in the Supreme Court's understanding of what privacy means and ought to mean. The Court treats privacy almost as if it were a "discrete commodity, possessed absolutely or not at all". Yet what could be more commonplace than the idea that it is up to the individual to measure out information about herself selectively – to whomever she chooses? ... A majority of Justices apparently confuse privacy with secrecy; yet even their notion of secrecy is a strange one, for a secret remains a secret even when shared with those one selects for one's confidences.

97 429 US 589 (1977).

98 See Schwartz 1989 *Am J Comp L* 675, 681. Also see Kang 1998 *Stanford LR* 1193, 1230 fn 157. The *Whalen* case is considered by Devenish *SA Bill of Rights* 143 to be "the most jurisprudentially sound decision of the [US] Supreme Court in relation to privacy".

The court rejected the plaintiffs' challenge, but only after carefully balancing the individuals' interests, protected by the right of limited disclosure, against the state's justification for intruding upon those interests. The court identified two interests as being involved in cases "sometimes characterised as protecting 'privacy'", namely:

- the individual's interest in avoiding disclosure of personal matters
- the interest in independence in making certain kinds of important decisions[99]

The court upheld the statute as a rational legislative attempt to deal with a problem of vital local concern, namely the diversion of the drugs involved to illegal uses. The statute did not pose a sufficiently serious threat to either the privacy interest in avoiding disclosure of personal matters, or the privacy interest in independence in making important decisions for the court to strike it down. Any privacy interests that the users of the drugs might have had in the information gathered by the state were outweighed by the state's interest in gathering the information.[100]

It is important to note, however, that the court did not decide any question that may be raised by the unwarranted disclosure of accumulated private data, or by a system that did not contain strong security provisions. *Dicta* by Justices Stevens and Brennan suggest that they were aware of the threats posed by computerised data systems and that they might consider disclosure of such data to be a violation of a constitutionally protected privacy interest.[101]

---

99 *Whalen v Roe* 429 US 589 (1977) 598–600. See Schwartz 1995 *Iowa LR* 553, 574 *et seq* for a discussion of subsequent decisions of lower courts in which *Whalen* was applied. Also see Hosch 1983 *Vand LR* 139; Mowery 1998 *U Cin LR* 697, 703 *et seq*; Komuves 1998 *J Mar J Computer & Inf L* 529, 561.

100 According to Hosch 1983 *Vand LR* 139, 191 the court did not apply strict scrutiny (ie requiring the showing of a "compelling state interest" before the statute will be upheld) as it usually does when a fundamental interest is involved, but nevertheless applied a "heightened rational basis examination" of the type the court uses when scrutinising interference with non-fundamental rights of constitutional dimension in the equal protection context. He further points out that the Supreme Court continued this trend in *Nixon v Administrator of General Services* 433 US 425 (1977). In this case former President Nixon claimed that his constitutional privacy right was violated by the Presidential Records and Materials Preservation Act which authorised the General Services Administrator to take custody of his papers and tapes for subsequent screening by government archivists. The court rejected his argument, deciding that the statute had been carefully drafted to minimise privacy intrusions and was designed to serve important national interests asserted by Congress.

101 Stevens J said:

(continued...)

According to Cate,[102] although the Supreme Court has never decided a case in which it found that a government regulation or action violated the constitutional privacy right created in *Whalen*, a number of federal appellate and district courts have done so.[103]

Another case that furnishes "grounds for optimism with respect to informational privacy",[104] apart from *Whalen*, is *Department of Justice v Reporters Committee for Freedom of the Press*.[105] The *Reporters Committee* case also involved the individual's interest "in avoiding disclosure of personal matters". The case arose out of requests made by the respondents under the Freedom of Information Act (FOIA) of 1966[106] for information concerning the criminal records ("rap sheets") of four members of the Medico family. The Department of Justice denied disclosure of the records, relying on exemption 7(C)[107] of the FOIA, which excludes records or information compiled for law enforcement purposes to the extent that the disclosure could "reasonably be expected to constitute an unwarranted invasion

101(...continued)

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed...

Whalen v Roe 429 US 589 (1977) 605.

Brennan, J was even more explicit:

> The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology...

Whalen v Roe 429 US 589 (1977) 607.

102 Cate *Information age* 63.

103 Cate *Information age* 63 cites *Tavoulareas v Washington Post Company* 724 F 2d 1010 (DC Cir 1984) (*inter alia* finding that corporations also possess constitutionally protected privacy rights – at 1022); *Barry v City of New York* 712 F 2d 1554, 1559 (2d Cir 1983); *Schacter v Whalen* 581 F 2d 35, 37 (2nd Cir 1978); *Doe v Southeastern Pennsylvania Transportation Authority* 72 F 3d 1133 (3rd Cir 1995); *US v Westinghouse Electric Corporation* 638 F 2d 570, 577 (3rd Cir 1980); *Plante v Gonzalez* 575 F 2d 1119 1123 (5th Cir 1978); *Doe v Attorney General* 941 F 2d 780, 795–797 (9th Cir 1991).

104 Flaherty 1991 *Case West Res LR* 831, 840.

105 489 US 749 (1989).

106 Codified at 5 USC s 552 (see par 4.2.4).

107 5 USC s 552(b)(7)(C) (see par 4.2.4).

of personal privacy". The respondents contended that the Medicos had no privacy interest in avoiding disclosure of "rap sheets" compiled by the federal government, because the events (arrests, indictments, convictions, and sentences) summarised in a "rap sheet" have been previously disclosed to the public. The court rejected the respondents' "cramped notion of personal privacy":[108]

> To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few factors that are not at one time or another divulged to another. Thus the extent of the protection accorded privacy at common law rests in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a person or group or class of persons: not freely available to the public." [See Webster's *Third New International Dictionary* 1804 (1976)...][109] Recognition of this attribute of a privacy interest supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole... the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interests implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information...

The court also emphasised the role of the computer in compiling information:

> The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and

108 *Dept of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989) 763–764.

109 References in a footnote to the definitions of privacy given by Westin *Privacy and freedom* 7 and other writers are omitted from the quotation. See *Dept of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989) 764 fn 16.

> store information that would otherwise have surely been forgotten long before a person attains the age of 80, when the FBI rap sheets are discarded.

In the end the court concluded that the purpose of the FOIA is to ensure that the government's activities are laid open to public scrutiny, and not that information about private citizens that happens to be in the warehouse of the government be disclosed.[110] Accordingly appellants' reliance on the exemption was upheld.

According to Flaherty,[111] the *Reporters Committee* case, although dealing specifically with the interpretation of an exemption to the FOIA, is very important for informational privacy, since it identifies and confirms the individual's interest in informational privacy. This case may also suggest the direction the Supreme Court will follow in future cases involving the individual's interest in informational privacy.[112] Where the Supreme Court had previously required that the information in records should be intimate, personal information, such as health or family information, and that it should have been held in strict confidence before the court was prepared to recognise that the individual had a privacy interest in the information, the *Reporters Committee* case found that there is an expectation of privacy in a computerised, comprehensive record of all an individual's activities, but not necessarily an expectation of privacy with regard to a single criminal event.[113]

---

110 *Dept of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989) 774.

111 Flaherty 1991 *Case West Res LR* 831, 840–841.

112 Flaherty 1991 *Case West Res LR* 831, 840 argues that Stevens J came close to relying on "informational self-determination" as recognised by the German Constitutional Court in the 1983 "Census" decision. For a comparative analysis of US constitutional protection of information privacy as opposed to the approach in Germany, see Schwartz 1989 *Am J Comp L* 675 *et seq*; Daniel-Paczosa 1987 *Arizona J Int Comp L* 154–163. For a discussion of the Census decision, see Simitis 1984 *NJW* 398–405; Riedel 1984 *Human Rights LJ* 67–75; Oliver & Von Borries 1984 *Pub L* 199–206; Weichert 1992 *Computer und Recht* 738–745.

113 Belair "Redefining information privacy" 1989 *Privacy Journal* 7 (quoted in Flaherty 1991 *Case West Res LR* 831, 841).

4 PROTECTION OF DATA PRIVACY BY MEANS OF LEGISLATION

4.1 Introduction: brief overview of legislation in public and private sectors

Legislation protecting data privacy in the USA is sectoral; American policy makers prefer to deal with data privacy issues as and when they become a problem. A specific event usually "triggers" the legislation process.[114] It should also be borne in mind that the USA is a federation of states. Privacy issues are within the domain of the states,[115] but Congress also has legislative power in this area.[116] Although the different states may also have legislation in place,[117] only the federal legislation affecting data protection will be discussed.[118]

---

114 See fns 121, 127, 135, 142.

115 See eg *Katz v US* 389 US 347, 350–351 (1967):

> [P]rotection of a person's *general* right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States.

116 Congressional authority to regulate at the state level is based on the commerce clause, US Const art 1 s 8, which provides:

> The Congress shall have Power ... To regulate commerce with foreign Nations, and among the several States ...

Since most computer data bases operate within interstate commerce, Congress has the power to legislate in this area.

117 There is eg no omnibus legislation at federal level dealing with data privacy in criminal records. The Crime Control Act of 1973 (42 USC s 3701) requires state criminal justice information systems developed with federal funds to be protected by measures that ensure the privacy and security of the information in the system. However, each state is expected to develop programs to manage and protect its criminal justice information. As a rule in state legislation in this area, individuals may inspect their own criminal arrest records (see eg the California Health and Safety Code s 11361.5 and the California Penal Code s 851.6(b)). Some state legislation also provides for the criminal records to be destroyed if a person was arrested, indicted or otherwise charged, but was later acquitted, pardoned or not prosecuted (see eg Connecticut General Statute Annotated s 54–142a; Florida Statute Annotated s 901.33). See in general Smith *Compilation* 3–5. Also see Goldstein 1992 *Emory LJ* 1185 who identifies three state models after an analysis of data protection legislation.

118 For a useful compilation of the texts of the Acts discussed, see Rotenberg *The privacy law sourcebook 1999*.

4.1.1 Legislation in public sector

The most important piece of legislation protecting privacy of personal information in the public sector is the Privacy Act of 1974. This Act was enacted to control the personal information practices of federal government agencies. It will be discussed in detail below.[119]

Other pieces of legislation that aim to protect the individual's privacy in respect of personal information against the federal government are:

- **Family Educational Rights and Privacy Act (FERPA) of 1974**[120]

This Act regulates government's (and other individuals') access to personal education records.[121] The purpose of FERPA is to allow access to educational records by students and parents while protecting the confidentiality of such records.[122] As a general rule, schools may not release school records or any other personally identifiable information without the prior consent of the student.[123] In contrast to other legislation in the privacy field, FERPA does not afford private remedies to the

119 See par 4.2.

120 Pub L No 93–380, 88 Stat 571 (1974); codified at 20 USC s 1232g. FERPA is popularly known as the "Buckley Amendment" after its patron Senator James Buckley of New York (see Hixon *Public society* 219).

121 The stimulus for the passage of FERPA was a study done in 1974 by the National Council of Citizens in Education (NCCE) entitled *Children, parents, and school records.* In its report, the NCCE identified several abuses in elementary and secondary school record keeping, such as *carte blanche* access to school records by school personnel, law enforcement agencies, welfare and health department workers; denial of the right of parents and students to inspect school records, to control what goes into them, and to challenge their contents; failure to obtain permission from parents before collecting information on students and their families; serious abuses in the preparation of student records that follow students throughout their educational careers; failure to inform students and parents when, to whom, and why others are given access to records.

122 *Student Press Law Center v Alexander* 778 F Supp 1227 (DDC 1991); Menacker *School law* 270 sees the purpose much wider:

> The purpose of the Family Rights and Privacy Act was to protect students against abuses of their welfare caused by the school's unrestricted control of student records.

123 Peer grading, the practice of allowing a fellow student to score a test, and the reporting aloud of peer grades was held not to violate FERPA by the Supreme Court in *Board of Education v Earls* 122 S Ct 2559 (2002).

individuals it protects.[124] Compliance with its provisions is ensured by denying federal funds to educational agencies that establish "a policy or practice" that contravenes the provisions of FERPA.[125]

❒ Right to Financial Privacy Act (RFPA) of 1978[126]

This Act regulates federal access to individual financial records.[127] The RFPA is designed to protect the customers of financial institutions from unwarranted intrusion into their records by the federal government, while at the same time permitting legitimate law enforcement activity. It "seeks to strike a balance between customers' right of privacy and the need of law enforcement agencies to obtain financial records pursuant to legitimate investigations".[128] As a general rule a financial institution may not disclose information contained in a customer's financial record to a government authority.[129] However, if certain procedural requirements are met,[130] or if one of the specific exceptions apply,[131] it may release such information.[132] The Act does not impose restrictions on private sector access to individual bank

124 See eg *Conzaga University v Doe* 122 S Ct 2268 (2002).

125 On FERPA, see in general Roos 1990 *TSAR* 477, 487; Menacker *School law*; Hudgins & Vacca *Law and education*; Drebes 1994 *JL & Education* 290; Cate *Information age* 87–88; Dagget 1997 *Catholic ULR* 617.

126 Pub L 95–630. Codified at 29 USC s 3401 *et seq*.

127 The RFPA was enacted after the decision by the Supreme Court in *US v Miller* 425 US 435 (1976) (see fn 94).

128 HR Rep No 1383, 95th Cong, 2d Sess 33, reprinted in 1978 US Code Cong & Ad News 9273, 9305.

129 12 USC s 3402, 3403(a),(b).

130 12 USC s 3402. Financial information may be disclosed if the financial records are reasonably described and the customer has either authorised the disclosure, or the agency has obtained an administrative or judicial subpoena, or a search warrant, or makes a formal written request that complies with the requirements of the RFPA.

131 12 USC s 3413. Disclosure of financial information is not prohibited if the information is not "identified with or identifiable as being derived from" the records of a particular customer, or if its disclosure is otherwise authorised by law. A government authority need not comply with the notice requirements of the RFPA if it is, pursuant to a law enforcement activity, seeking only the name, address, account number and type of account "of any customer or ascertainable group of customers associated with a financial transaction or class of financial transactions".

132 See also Roos 1990 *TSAR* 477, 482–486; Rogovin 1986 *Ann Surv Am L* 587 *et seq*; Petrocelli *Low profile* 24; Hixon *Public society* 220; Gross *Privacy* 30.

records.[133]

❒ Privacy Protection Act (PPA) of 1980[134]

This Act was designed to control government searches of newsrooms and is mainly concerned with interference with First Amendment rights during search and seizure of documentary material by law enforcement agencies.[135] The PPA protects the privacy of the home or workplace of a "person reasonably believed to have a purpose to disseminate to the public ... a form of public communication"[136] by limiting the ability of law enforcement agencies to search for documentary materials by using a search warrant only. Any action by a law enforcement officer in contravention of the PPA is unlawful,[137] and an aggrieved person has a cause of action for damages.[138] However, an officer or employee who had a reasonable *bona fide* belief in the lawfulness of his conduct has a complete defence.[139]

133 Until 1999, the banking industry relied on self-regulation (see Schwartz & Reidenberg *Data privacy law* 262). The Gramm-Leach-Bliley Act now regulates private sector access to financial records. See further below.

134 Pub L No 96–440, Title I s 101, 94 Stat 1879, s 106, 94 Stat 1880, s 107, 94 Stat 1881; codified at 42 USC s 2000aa.

135 The PPA was the Congressional response to the Supreme Court's holding in *Zurcher v Stanford Daily* 436 US 547 (1978) that the Fourth Amendment does not confer any special protection upon the possessor of documentary evidence (*in casu* a student newspaper) against search and seizure where such possessor is not a suspect in the investigation, but may have material in his or her possession that could help the police in their investigations. Eckenweiler 1998 *Seton Hall Const LJ* 725, 730 argues that the PPA can be extended to protect material intended for publication on the Internet.

136 42 USC s 2000aa(a).

137 42 USC s 2000aa(a), (b).

138 42 USC s 2000aa-6 (a). Actual damages can be awarded as well as reasonable attorney and litigation costs (s 2000aa-6(f)). The cause of action is extended against the United States, a state that has waived its governmental immunity, or an officer or employee of a state that has not done so (s 2000aa-6(a)).

139 42 USC s 2000aa-6(b).

❒ Computer Matching and Privacy Protection Act (CMPPA) of 1988

This Act was enacted to amend the Privacy Act of 1974 to control computer matching.[140]

❒ Driver's Privacy Protection Act (DPPA) of 1994[141]

The DPPA prohibits Departments of Motor Vehicles (DMV) and their employees from releasing personal information from any person's driver's record unless the request falls within any of fourteen exemptions.[142]

❒ Health Insurance Portability and Accountability Act (HIPAA) of 1996[143]

The HIPAA, also known as the Kassebaum-Kennedy Act, was introduced *inter alia* to regulate the privacy of personal health care information.[144] The Act requires the Secretary of Health and Human Services to submit to Congress detailed recommendations on the rights that an individual, who is a subject of individually identifiable information, should have; the procedures that should be established for the exercise of such rights; and the uses and disclosures of such information that should be authorised or required.[145] The Act further mandates the Secretary to promulgate regulations that would create standards for health data maintained electronically if Congress failed to pass legislation governing

140 The CMPPA is discussed with the Privacy Act (see fn 270 and accompanying text).

141 Pub L 103–322, 108 Stat 2099–2102 (1994) codified at 18 USC s 2721 (1997).

142 The "trigger" for this legislation was the death of actress Rebecca Schaeffer, who was killed by an obsessed fan who obtained her address from her California Department of Motor Vehicle record (see Cate *Information age* 79; Regan *Legislating privacy* 102–103; Alderman & Kennedy *Right to privacy* 325). The constitutionality of this Act was upheld by the Supreme Court in *Reno v Condon* 528 US 141 (2000). In an unanimous decision, the court found that the information in the records held by state motor vehicle agencies was "an article of commerce" and can be regulated by the federal government.

143 Pub L 104–191, 110 Stat 1936 (1996) codified at 42 USCA s 1320.

144 Other aims of the HIPAA include improving "portability and continuity" of health insurance and combatting waste and fraud in health insurance and health care delivery.

145 These recommendations were presented in 1997. For a discussion, see Carter 1999 *William Mitchel LR* 223, 271–285.

such standards.[146] Since Congress failed by August 1999 to pass such legislation, the Secretary published draft rules in November 1999 and the final rules in December 2000. EPIC[147] is critical of these regulations:

> The large number of exemptions provided limits the protection offered by the new rules. For example, patients' information can be used for marketing and fundraising purposes. Doctors, hospitals, and health services companies will be able to send targeted health information and product promotions to individual patients and there is no opt-out right to limit this marketing use of medical data.

4.1.2 Legislation in private sector

The United States has no comprehensive privacy protection law for the private sector. The various federal laws that protect certain specific categories of personal information, have been described as "a patchwork" of laws[148] and "haphazard".[149] The Fair Credit Reporting Act (FCRA) of 1970 was Congress's first attempt to protect the privacy of consumers, and predates the Privacy Act of 1974. This Act will be discussed in detail.[150] Other statutes that are worth mentioning are:

---

146 For a discussion of HIPAA, also see Barefoot 1998 *N Car LR* 283; Gilbert 1997 *N Dakota LR* 93, 95 *et seq*; Shalala 1998 *Health Matrix* 223, 224; Woodward 1997 *J L Med & Ethics* 88.

147 EPIC *Privacy and human rights* 386.

148 EPIC *Privacy and human rights* 385; Gellman 2000 *Gov Inf Q* 235, 237; Jay & Hamilton *Data protection* 132.

149 Blackman 1993 *Santa Clara Computer & High Tech LJ* 431, 456 points out that the result of this piecemeal approach to personal data protection is that it makes it impossible for an individual to know his or her privacy rights. It is also difficult to know which industries are controlled and which are not. Eg: if a consumer orders video tapes from a mail order company, his or her records on this order will be protected (by virtue of the Video Privacy Protection Act (see fn 165)), but there will be no protection if the order is for lingerie. The irony of the law as it was then was that there was more protection for video rental information than for more sensitive matters such as health care information (see Mowery 1998 *U Cin LR* 697, 732; Shalala 1998 *Health Matrix* 223, 224).

150 See par 4.3.

❒ Cable Communications Policy Act (CCPA) of 1984[151]

The CCPA includes measures to protect the privacy of subscribers to cable television. It restricts the collection, storage and disclosure of personally identifiable information without the subscriber's consent[152] and requires that service providers provide their subscribers with access to information collected about them.[153] The Act also requires the cable service provider to inform the customer at least once a year of the information it collects, the nature, frequency and purpose of any disclosure of that information, the duration of its storage, the times and places at which a customer may have access to that information, and the terms of the statute.[154] The CCPA provides for statutory damages against cable operators who violate their customers' rights under the Act.[155] The Act includes some exemptions, particularly for disclosures of information "necessary to render, or conduct a legitimate business activity related to" the provision of cable service.[156] According to Cate,[157] the CCPA constitutes the broadest set of privacy rights in any federal statute.

❒ Electronic Communications Privacy Act (ECPA) of 1986[158]

The ECPA prohibits the interception or disclosure of the contents of any electronic communication, such as telephone conversations or e-mail, or even of any conversation in which the participants exhibit "an expectation that such communication is not subject to interception under circumstances justifying

151 Pub L 98–549; codified at 47 USC s 551.

152 47 USC s 551(c).

153 47 USC s 551(d).

154 47 USC s 551(a)(1).

155 47 USC s 551(f).

156 47 USC s 551(c).

157 Cate *Information age* 86.

158 Codified at 18 USC ss 2510–2520, 2701–2709. For a discussion of the ECPA, see Hernandez 1988 *Fed Com LJ* 17–41. Also see Reidenberg & Gamet-Pol 1995 *Wake Forest LR* 105, 114–115.

such an expectation."[159] Cate[160] points out that this apparently broad privacy right is riddled with exceptions, the most significant of which is that the prohibition does not apply if a party to the communication consents to disclosure.[161] The prohibition also does not apply to switchboard operators, employees of telecommunications service providers, employees of the Federal Communications Commission, or anyone assisting the holder of a warrant, provided they are acting within the scope of their duties.[162] Furthermore, the prohibition does not apply if the communication intercepted was "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public, including any marine or aeronautical system, amateur and citizens band radio, or general mobile radio services".[163]

The ECPA applies only to the interception or disclosure of the contents of any electronic communication; it does not apply to "transactional" information, so service providers are not restricted by this Act as regards the collection, storage or disclosure of such data. In fact, the statute explicitly authorises the use of "a pen register or a trap and trace device" to record information about other individuals' conversations or transmissions.[164]

❒ Video Privacy Protection Act of 1988[165]

This Act, also known as the Bork Act,[166] seeks to protect the records of individual borrowers held by

159 18 USC s 2510–11.

160 Cate *Information age* 84.

161 18 USC s 2511(2)(c).

162 18 USC s 2511.

163 18 USC s 2511(2)(g).

164 See Cate *Information age* 85. This gap was filled by the Telecommunications Act of 1996, discussed below.

165 Pub L No 100–618, 102 Stat 1395 (1988) codified at 18 USC s 2710.

166 This Act was adopted in response to congressional outrage over the disclosure of the list of videos rented by Judge Robert Bork during his ill-fated Supreme Court nomination confirmation hearings - see Cate *Information age* 86. A Washington newspaper published a profile of Judge Bork in September 1987, based (continued...)

video tape rental stores. It provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided ...." The statute also requires the destruction of personally identifiable information not later than one year after the information is no longer necessary for the purpose for which it was collected.[167] There are significant exemptions, for example, if the disclosure is incidental to the ordinary course of business of the video tape service provider.[168] Data about user viewing habits may also be disclosed for marketing purposes if the user has been given an opportunity to "opt out" of such disclosure.[169] As a result, lists are widely available that contain information on user viewing habits and other demographic information, such as median age and income.[170]

❒ Telecommunications Act of 1996[171]

This Act contains provisions protecting the privacy of "Customer Proprietary Network Information" (CPNI). The Act defines CPNI as "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue

166(...continued)
on 146 films his family had rented from a video store. At the time, the Senate Judiciary Committee was conducting hearings on the judge's nomination to the Supreme Court. Although the list of videos included nothing to draw national attention, Senators and Congressmen were stunned by what they regarded as an invasion of privacy. The House and Senate quickly introduced legislation; after all, if the viewing habits of a judge were newsworthy, so were those of the members of Congress! See *New York Times* 27 Feb 1988 18. (It is interesting to note that Judge Bork's nomination did not succeed, principally because he refused to accept the principle of *Roe v Wade* 410 US 113 (1973) that privacy was implicitly protected by the Constitution.)

167 18 USC s 2710(e).

168 18 USC s 2710(b)(2)(E).

169 18 USC s 2710(b)(2)(D).

170 See Cate *Information age* 86.

171 Pub L 104–104; codified at 47 USC s 222.

of the carrier-customer relationship".[172] Under the Act, service providers may use, disclose or permit access to individually identifiable CPNI only if it is necessary to provide the telecommunications service from which the information is derived or other services necessary to render the telecommunications service.[173] Service providers are free to use CPNI as is necessary to protect their own business interests.[174]

❒ Children's Online Privacy Act of 1999[175]

This Act requires that the operator of a website or online service directed to children, should obtain parental consent before personal information is collected, via the Internet, from children under the age of thirteen years.[176] The Federal Trade Commission (FTC) is responsible for enforcing the Act.[177]

❒ Gramm-Leach- Bliley (GLB) Act of 1999[178]

The GLB Act eliminates traditional ownership barriers between different financial institutions such as banks, securities firms and insurance companies. Title V of GLB limits instances in which a bank or other financial institution may disclose "nonpublic personal information" about consumers to "nonaffiliated third parties". It also requires financial institutions to disclose to their retail customers the institution's privacy policies and practices with respect to information sharing. Title V also requires financial institutions to give consumers the opportunity to "opt out" of information sharing and to be informed of the procedures they could use to opt out.

---

172 47 USC s 222(f)(1).

173 47 USC s 222(c)(1).

174 47 USC s 222(d). See further Cate *Information age* 85.

175 Pub L 105–277; codified at 15 USC s 6501–6505.

176 15 USC s 6502.

177 15 USC s 6505.

178 Pub L 106–102; codified at 15 USC s 6801 *et seq*.

The general prohibition on sharing nonpublic personal information with non-affiliates does not apply to eight categories of disclosures. These include disclosures that are necessary to effect, administer or enforce a transaction requested or authorised by the consumer; disclosures that the customer has consented to; disclosures intended to prevent fraud or unauthorised transactions, to protect the confidentiality or security of the institution's records, for risk control or for resolving customer disputes or inquiries, and to persons holding a legal or beneficial interest relating to the customer or persons acting in a fiduciary or representative capacity on behalf of the customer; disclosures to the extent permitted or required by law and in accordance with the Right to Financial Privacy Act and to law enforcement agencies etcetera; disclosures for an investigation on a matter related to public safety; disclosures to consumer reporting agencies; and disclosures intended to comply with federal, state and local laws.[179]

❒ Conclusion

Privacy-related legislation remains a relevant topic in the US Congress, and each year several bills dealing with privacy issues are introduced into the House or the Senate.[180] The Clinton administration also recognised the importance of privacy in the information era.[181] In the wake of the terrorist attacks

179 For a discussion of the GLB Act, see Flanagan 2002 *J Int Banking L* 237; Janger & Schwartz 2002 *Minn LR* 1219; Savino & Smirti 2000 *Banking LJ* 7; Horn & Smith 1999 *Banking LJ* 689.

180 Eg, in 1998 (105th Congress) and 1999 (106th Congress) over 100 bills dealing with privacy protection were pending in Congress; these included laws on genetic and medical records, Internet privacy, and children's rights (see GILC *Privacy and human rights* 24). (Bills and Acts of the US Congress can be found on the website of the Library of Congress: see http://thomas.loc.gov.)

According to Regan *Legislating privacy* 103, the biggest information privacy issue in the 1990s involved medical information. For more detail on this issue, see Gostin 1995 *Cornell LR* 451; Schwartz 1995 *Vand LR* 295; Turkington 1997 *JL Med & Ethics* 113; Schwartz 1997 *Tex LR* 1; Rothstein *Genetic secrets.* Privacy on the Internet or in "cyberspace" will probably dominate the privacy debate in the next decade (see Kang 1998 *Stanford LR* 1193; Schwartz 1999 *Vand LR* 1609).

181 The Clinton administration has focused considerable attention on the value of the national and global information infrastructure. President Clinton and Vice-President Gore created the Information Infrastructure Task Force (IITF), which has a Privacy Working Group which is responsible for addressing privacy issues posed by the proliferation of electronic information networks (see Cate *Information age* 91). The IITF has produced a document called Options for Promoting Privacy on the National Information Infrastructure (1997), inviting public comment in order to develop consensus regarding the appropriate allocation of public and private sector responsibility for implementation of fair information practices.

on 11 September 2001, the Bush administration passed the USA Patriot Act of 2001.[182] This Act significantly weakened privacy protection in federal wiretapping statutes.[183]

In 2002, Senators Joe Lieberman and Conrad Burns introduced the E-government Act. This Act requires federal government agencies to conduct "privacy impact assessments" before developing or procuring information technology or initiating any new collections of personally identifiable information. The privacy assessment must address what information is to be collected, why it is being collected, the intended uses of the information, with whom the information will be shared, what notice will be provided to individuals and how the information will be secured.[184]

4.2 Privacy Act of 1974

4.2.1 Background and legislative history

4.2.1.1 Introduction

In the United States, as in European countries,[185] proposals for the establishment of a centralised data bank, plans to mandate the extensive use of a personal identifier (PIN), an impending census, and alarmist writings by privacy advocates during the late 1960s and early 1970s led to the adoption of the Privacy Act in 1974. Political events of the time, especially the Watergate scandal, also played a significant role.

4.2.1.2 Congressional and executive investigations

The threat posed to personal privacy by the computer came to public notice partly as a result of the

182 Pub L 107–56.

183 Also see EPIC *Privacy and human rights* 390.

184 See http://www.cdt.org/legislation/107th/e-gov/.

185 See eg the UK (ch 4 par 4.2.1.1) and the Netherlands (ch 5 par 4.2.1).

proposed establishment of a central data bank in the 1960s. In 1966 the Social Sciences Research Council proposed the establishment of a Federal Data Centre with the authority to obtain computer tapes and other machine-readable data produced by all federal agencies. Its function would have been to provide data and service facilities to federal agencies and users outside the government.[186] This proposal prompted investigation by both the Senate[187] and the House of Representatives. A special Subcommittee on Invasion of Privacy was created by the House of Representatives' Committee on Government Operations, which held hearings in this regard,[188] culminating in a report which appeared in 1968.[189] In the end the proposed Central Data Bank floundered amid a spate of hostile publicity.[190]

The 1970 census also aroused public disquiet because of the intrusiveness and extensiveness of the questions. Congressional investigations of the Bureau of Census prompted the Bureau to take measures to restore public and legislative confidence.[191]

A Congressional threat to mandate the universal use of the social security number as a personal identifier in 1972 led the Secretary of Health, Education and Welfare to establish an Advisory Committee on Personal Data Systems to analyse the consequences of using computers to keep records about people. The committee released its report *Records, computers and the rights of citizens* in 1973.[192] The report noted the growth in automated record keeping and accepted the need for safeguards for privacy. It recommended that a Code of Fair Information Practices be enacted for all

186 Bennett *Regulating privacy* 46; Regan *Legislating privacy* 8.

187 US Senate *Government Dossier* Report from the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, Senate, 90th Congress, 1st Sess (1967).

188 For more details on these hearings, see Regan *Legislating privacy* 72.

189 US House of Representatives Hearings before the Special Subcommittee on Invasion of Privacy: *Special inquiry on invasion of privacy* part 1 June and Sept 1965, part 2 May 1966; *The computer and invasion of privacy* July 1966; *Privacy and the National Data Bank concept* Aug 1968.

190 Bennett *Regulating privacy* 74; Regan *Legislating privacy* 7.

191 Bennett *Regulating privacy* 52.

192 US Dept of Health, Education, and Welfare: *Records, computers and the rights of citizens*, report of the Secretary's Advisory Committee on Automated Personal Data Systems (1973).

automated personal data systems. The Code rested on five basic principles:[193]

- There must be no personal data record keeping systems of which the very existence is secret.
- Individuals must have some means of finding out what information about them is on record and how it is used.
- Individuals must have some means of preventing information about them that was obtained for one purpose from being used or made available for other purposes without their consent.
- Individuals must have some means of correcting or amending a record of identifiable information about them.

The report also recommended that individuals should be able to refuse to disclose their social security number to organisations not authorised by the federal government to collect or use it.[194]

The work done by the Senate Judiciary Committee's Subcommittee on Constitutional Rights, chaired by Senator Sam J Ervin Jr, from 1970 to 1974, had a very important influence on the subsequent passage and content of the Privacy Act.[195] During this period the subcommittee heard testimonies from the computer industry on possible abuses of computerised information systems and analysed the issue

193 *Records, computers, and the rights of citizens* 41. In 1994, the Privacy Working Group of the IITF (see fn 181) issued draft principles intended to update this Code for the 1990s. The Working Group pointed out that the Code was intended for a paper-based society. With the envisaged National Information Infrastructure of the 1990s and beyond, consumer electronics put information at users' fingertips. The traditional fair information practices should be adapted to this new environment where information and communications are sent and received over networks. The new "Principles for Providing and Using Personal Information" are intended to be equally applicable to public and private entities, and are intended to be a framework from which specialised principles can be developed. The Principles involve general principles (which include an information privacy principle and an information integrity principle); a collection principle for information collectors; principles for information users (which entail an acquisition and use principle, a protection principle, an education principle and a fairness principle); and principles for individuals who provide information (which entail an awareness principle, and a redress principle). For the text of the "Principles for Providing and Using Personal Information" see 1994 (May / June) *TDR* 43–45.

194 *Records, computers, and the rights of citizens* 126.

195 See Regan *Legislating privacy* 75; Bennett *Regulating privacy* 69.

of federal data banks.[196] Its report *Federal data banks and constitutional rights* was published in 1974 and became very influential. It concluded that there were immense numbers of government data banks, permeated with diverse information on almost every citizen in the country. It recommended that the existence, creation and operation of data banks should be put on a statutory footing with full and accurate reporting requirements, inherent privacy safeguards, subject notification, constraints on interagency exchange, and strict security precautions – in other words, "continued legislative control over the purpose, contents, and uses of government data banks".[197]

4.2.1.3 Computer and privacy literature

Congressional and executive office investigations were accompanied by "computer and privacy" literature such as *The naked society* by Vance Packard (1964), *The privacy invaders* by Myron Brenton (1964), Alan Westin's *Privacy and freedom* (1967) and Arthur Miller's *Assault on privacy* (1971). This literature tried to raise public awareness of the intrusiveness of new technologies. There are numerous references to "Big Brother" and "1984"in this literature.[198]

4.2.1.4 Political climate

In consequence of congressional and other hearings and literature on the subject of privacy, numerous bills concerning personal privacy were filed in both the Senate and the House. During the period 1965 to 1972 (89th–92nd Congresses) no less than 271 different legislative bills relating to privacy were introduced.[199] This was partly due to the tense political climate that had prevailed since the late

196 US Senate *Federal data banks, computers, and the bill of rights*, hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, Senate, 92nd Cong, 1st Sess (1971).

197 US Senate *Federal data banks and constitutional rights*, report of the Subcommittee on Constitutional Rights of the Committee on the Judiciary, Senate, 93d Cong 2d Sess (1974) iv–v (quoted in Bennett *Regulating privacy* 69).

198 Bennett *Regulating privacy* 70. Also see Farnsworth 1983 *Int Bus L'yer* 114.

199 Bennett *Regulating privacy* 69. But only two laws were enacted that directly addressed the issue: the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC 2510–2520) (limiting the use of wiretaps) and (continued...)

1960s.[200] Revelations during the Watergate investigations gave further urgency to the adoption of legislation to protect individual privacy.[201] Many commentators believe that the Privacy Act would not have been passed if it had not been for Watergate.[202]

4.2.1.5 Passage of Privacy Act

Both Houses of Congress wanted some sort of privacy legislation to be in place before the end of the 1974 session. Consequently, the consideration and passage of the Privacy Act were, according to Bennett,[203] astoundingly quick by American standards. The Senate Bill (S 3418), mainly sponsored by Senator Ervin, and the House Bill (HR 16373) were passed in November of that year. The Senate Bill provided for the establishment of a Federal Privacy Board to oversee the collection, use and disclosure of information concerning individuals, whereas the House Bill did not propose such a privacy board or any other separate mechanism to enforce privacy principles. A compromise had to be struck before the Bill could become law.[204] Two compromises were reached: the Federal Privacy Board was transformed into a Privacy Protection Study Commission,[205] a temporary body with advisory and analytical responsibility only; and the oversight responsibility was given to the Office of Management

(...continued)
the Fair Credit Reporting Act of 1974 (15 USC 1681 *et seq*) (regulating credit agencies – see par 4.3).

200 The assassination of Robert Kennedy and Martin Luther King and the Vietnam war produced an increase in official surveillance and in congressional investigation into that surveillance (Bennett *Regulating privacy* 68).

201 US Senate *Legislative history of the Privacy Act* Government Operations Committee Rep No 1183, 93rd Cong, 2nd Sess (1974) 6926.

202 See Regan *Legislating privacy* 8. According to Bennett *Regulating privacy* 72, Watergate provided an "open policy window", ie a climate of public and political opinion that was propitious for action. The many and various cases of political bribery, corruption, malpractice, intrusiveness, and abuse of personal data that are captured by the emotive term "Watergate" gave the privacy advocates the perfect horror story, and pushed the whole problem of the executive abuse of power, vis-à-vis the Congress, the courts, and the citizen, to the forefront of press and public attention.

203 Bennett *Regulating privacy* 72.

204 For more detail on the interesting process followed in reaching this compromise, see Bennett *Regulating privacy* 73; Messick 1985 *Santa Clara LR* 153, 166 fn 60; O'Reilly *Federal information* par 20–03.

205 See par 4.2.5.

and Budget on the grounds that this duty was better placed within the Executive Office of the President than in a cabinet department (such as the Justice Department). The Bill was passed in both Houses on 18 December 1974 and was signed by President Ford on 1 January 1975.[206]

4.2.2 Provisions of Privacy Act[207]

4.2.2.1 Congressional findings

Section 2(a) of Public Law 93–579[208] sets out the Congressional findings, namely that

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

206 Bennett *Regulating privacy* 72. According to Bouchard *Guidebook* 45 the final enactment of the statute ended what was "an outstanding demonstration of legislative chaos", and the result of this "hasty and haphazard legislative process" is "an internally inconsistent statute with no reliable indication of congressional intent".

207 Pub L No 93–579, 88 Stat 1896 1974, referred to as the Privacy Act of 1974, and codified at 5 USC s 552a.

208 Ie the Privacy Act – this section was not codified as part of 5 USC s 552a.

4.2.2.2 Purpose of Privacy Act

The Privacy Act has three broad goals, namely:

- ❒ to recognise individuals' interests in government records concerning them
- ❒ to regulate the information practices of federal agencies
- ❒ to strike an appropriate balance between the need of individuals for a maximum degree of privacy regarding personal information they furnish to the government, and that of the government for information about the individual which it finds necessary in order to carry out its legitimate functions[209]

4.2.2.3 Scope of Privacy Act

a Relationship with other legislation

The Privacy Act 1974 enjoys the same status as other federal legislation. The Freedom of Information Act of 1966 is especially relevant here, and will be referred to later.[210] The provisions of other federal statutes, providing data privacy in areas not covered by the Privacy Act, have also been referred to.[211]

States may also legislate on the issue of privacy, and many states have enacted legislation protecting privacy in data banks in government.[212]

b Definitinal framework

Before individuals may enforce their right to privacy under this Act, the invasion of privacy must fall

209 Pub L 93–579 s 2(b); Bouchard *Guidebook* 44.

210 See par 4.2.4.

211 See par 4.1.

212 These statutes include provisions protecting public library records, vehicle registration records, and welfare records (see Smith *Compilation* 20–24).

within the definitional framework of the Act.

An analysis of the definitions of the Act shows that what the Act in essence protects is a **record**, in manual or automated form, on **an individual,** containing an identifying feature by means of which the individual can be connected to the information in the record, which must be **maintained** by a **federal agency** in a **system of records**, and which must be capable of being **retrieved** from that system of records by means of its identifying feature. The key terms in the definition are discussed below under separate headings.

i Agency

An agency is defined as any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the executive office of the President),[213] or any other independent regulatory agency.[214] The Act is only applicable to federal agencies,[215] but state agencies can be affected since information provided by a state agency to a federal agency will fall under the provisions of the Act.[216] Furthermore, states can be denied access to information held by the federal agency.[217] Information gathered and kept by state agencies themselves will, however, be excluded from the Act. The same is of course true of

213 However, those components of the Executive Office of the President whose sole function is to advise and assist the President are not "agencies" for purposes of the Privacy Act (see eg *Dale v Executive Office of the President* 164 F Supp 2d 22 (DDC 2001)).

214 5 USC s 552(f).

215 See, eg, *Perez-Santos v Malave* 23 Fed Appx 11 (1st Cir 2001); *Ditman v California* 191 F 3d 804 (9th Cir 1999). An exception to this rule is the social security number usage restrictions, contained in s 7 of the Privacy Act (Pub L 93–579), which apply to state and local government agencies as well (US Dept of Justice *Overview of the Privacy Act* 509).

216 According to Hosch 1983 *Vand LR* 139, 148–149 the Act is ambiguous about the entities that are subject to it, and the definition of an "agency" apparently depends on the function of the entity, not its organisational structure. Thus, a particular entity could use different definitions for varying functional purposes, providing for maximum free flow of information about individuals within that structure, while limiting the individual's access to the smallest possible number of files.

217 Sloan *Law of privacy* 18.

the information systems of private institutions.[218] It is therefore evident that the Privacy Act does not create obligations for the private sector,[219] but binds only the public sector (and only the federal part of the public sector, at that).

ii Individual

The Act only confers rights on "individuals" on whom a record is kept by a federal agency. An individual is defined as a citizen of the United States or an alien lawfully admitted for permanent residence.[220] In other words, the Act does not confer rights on foreign nationals without permanent residence in the US, or on juristic persons.[221] The Privacy Act also does not protect deceased persons.[222] Privacy Act rights are personal to the individual and cannot be asserted derivatively by others.[223] The parent of a minor or the legal guardian of an incompetent person may act on behalf of that individual.[224]

---

218 Government contractors and their employees are also subject to the Act (5 USC s 552a(m)(1)).

219 Private entities are not subject to the Act (see eg *Sutton v Providence St Joseph Med Ctr* 192 F 3d 826 (9th Cir 1999)). Federal funding does not render private entities subject to the Act *(Unt v Aerospace Corp* 765 F 2d 1440 (9th Cir 1985)).

220 5 USC s 552a(a)(2). See *Raven v Panama Canal Co* 583 F 2d 169 (5th Cir 1978).

221 See eg *St Michaels Convalescent Hosp v California* 643 F 2d 1369 (9th Cir 1981). But see *Recticel Foam Corp v US Dept of Justice* (No 98–2523, *slip op* at 11-15 (DDC Jan 31 2002), which produced the novel ruling that a corporation has standing to bring an action to enjoin an agency from disclosing investigative information on the company: "[T]he fact that Congress did not create a cause of action for corporations under the Privacy Act does not necessarily mean that Recticel's interests do not fall within the 'zone of interests' contemplated by that Act. It is sufficient for a standing analysis that Plaintiffs' interests 'arguably' fall within the zone of interests contemplated by the statute."

222 Flaherty *Surveillance societies* 355; OMB Guidelines 40 Fed Reg 28,948, 28,951; *Crumpton v US* 843 F Supp 751 (DDC 1994).

223 See eg *Parks v IRS* 618 F 2d 677 (10th Cir 1980) (court held that a union lacks standing to sue for damages on behalf of its members). But see *Nat Fed of Fed Employees v Greenberg* 789 F Supp 430 (DDC 1992) (court held that a union has associational standing because the members whose interests the union seeks to represent would themselves have standing).

224 See 5 USC s 552a(h); *Gula v Meese* 699 F Supp 956 (DDC 1988).

iii Record

The Privacy Act can only be relied on by individuals if a record is kept on them. The term "record" is defined as any item, collection or grouping of information about an individual that is maintained by an agency, including but not limited to, the individual's education, financial transactions, medical history and criminal or employment history. The information must also contain the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voice print or a photograph.[225] A record can therefore be contained either in a manual file or in an automated or computerised form, but the information in it must be linked in some way to the individual if it is to fall within the provisions of the Act.[226] Information which cannot be connected to an individual is not protected.[227]

iii Maintain

The record on the individual must be "maintained" by a federal agency. The term "maintained" is defined

225 5 USC s 552a(a)(4). See eg *Reuber v US* 829 F 2d 133 (DC Cir 1987). In *Albright v US* 632 F 2d 915 (DC Cir 1980) it was held eg that a videotape of a meeting that contains a means of identifying an individual by means of a picture or a recording of a voice, constituted a record for the purposes of the definition of the Privacy Act.

226 The Privacy Protection Study Commission (PPSC) established under the Privacy Act (see par 4.2.5) has recommended that the definition of "record" should be amended to include attributes and other personal characteristics assigned to an individual, and a new term "accessible record" should be defined to delineate those individually identifiable records that ought to be available to an individual in response to an access request. Accessible records would include those that, while not retrieved by an individual identifier, could be retrieved by an agency without unreasonably burdening it, either through its regular retrieval procedures or because the subject can help the agency find the record (eg because the person knows that he or she was mentioned in a document, though the agency does not normally access the record by reference to the person) (Privacy Commission Report 504).

227 Several courts of appeal have articulated tests for determining whether an item qualifies as a "record" under the Privacy Act, resulting in different tests for determining "record" status. See eg *Bechhoefer v US Dept of Justice Drug Enforcement Admin* 209 F 3d 57 (2d Cir 2000) (the term "record" encompasses any information about an individual that is linked to that individual through an identifying particular); *Boyd v Sect of the Navy* 709 F 2d 684 (11th Cir 1983) (in order to qualify as a "record" an item must contain information that actually describes the individual in some way) and *Tobey v NLRB* 40 F 3d 469 (DC Cir 1994) (in order to qualify as a "record" the information must both be about an individual and include his or her name or other identifying particular).

as including maintain, collect, use or disseminate.[228] It has been decided that this definition embraces various activities with respect to records and has a meaning that extends beyond the common usage of the term and includes the collecting of a record.[229]

iv System of records

The record on the individual must be maintained as part of a "system of records". This term is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some other identifying number, symbol, or other identifying particular assigned to the individual.[230] A "system of records" is therefore defined with reference to the means used to retrieve information from the system. This definition restricts the Act's scope in that information about an individual is only protected if it contains an identifying particular, and is retrieved from an information system by using this identifying particular.[231] In other words, coverage of the Act is made dependent upon the method of retrieval of a record rather than its substantive content.[232] Consequently, the Act fails to provide for the computer's ability to search for attributes, and to do textual searches without using a personal identifier.[233] The fact that the information must be contained in a system of

228 5 USC s 552a(a)(3).

229 *Albright v US* 631 F 2d 915 (DC Cir 1980). In *Albright* the scope of the term "maintain" was analysed in the context of subsection (e)(7), which prohibits an agency from maintaining records on First Amendment rights (see text to fn 320). The court held "the Act clearly prohibits even the mere collection of such a record".

230 5 USC s 552a(a)(5).

231 Eg, an employee was denied access to a memorandum of a meeting between him and his employer where the employer did not keep the information in a government system of records under the litigant's name or identifying number, but kept it randomly in a file from which it could only be retrieved by manually searching through the file (*Boyd v Sect of the Navy* 709 F 2d 684 (11th Cir 1983). Similarly, the publication of a letter containing the reasons for a public employee's discharge was held not to violate the Privacy Act, since the letter, which was in the Department of Education's system of records, was not retrievable by the employee's name or personal identifier (*McGregor v Greer* 748 F Supp 881 (DDC 1990)). Also see *Bechoefer v US Dept of Justice* 179 F Supp 2d 93 (WDNY 2001); Harrison 1992 *Memp SULR* 775, 797.

232 US Dept of Justice *Overview of the Privacy Act*.

233 Ehlke 1985 *J Mar LR* 829.

records has frustrated many litigants in their attempts to press Privacy Act claims.[234] [235]

v Summary

To sum up, the Privacy Act confers rights on individuals only (who must be citizens or permanent residents); it imposes obligations on government agencies (that is, the public sector) and it applies to records that may be contained either in a manual file or in an automated or computerised form, provided the information is in a system of records and is linked in some way to the individual concerned.

234 See eg *Am Fed of Gov Employees v NASA* 482 F Supp 281 (SD Tex 1980); *Chapman v NASA* 682 F 2d 526 (5th Cir 1982). See also Ehlke 1985 *J Mar LR* 829, 842. In *Thomas v US Dept of Energy* 719 F 2d 342 (CANM 1983), it was held that since this section expressly contemplates a "system of records" as the direct or indirect source of the information disclosed, this section does not prohibit the disclosure of information derived solely from independent sources although identical information may be contained in an agency's system of records. To make matters worse, courts have held that the agencies are not under an affirmative duty to place records within a system of records: see eg *Manuel v Veterans Admin Hosp* 857 F 2d 1112, 1119 (6th Cir 1988); *Wren v Heckler* 744 F 2d 86, 89 (10th Cir 1984). The PPSC was also critical of the "system of records" concept and recommended that the Act's definition of a system of records should be abandoned and its definition of a record amended. The Commission concluded (504) that the "system of records" definition has two limitations:

> First, it undermines the Act's objective of allowing an individual to have access to the records an agency maintains about him, and, second, by serving as the activating, or 'on/off switch' for the Act's other provisions, it unnecessarily limits the Act's scope.

On the PPSC, see also par 4.2.5.

235 However, the "system of records" threshold requirement is not necessarily applicable to all subsections of the Act. (See OMB Guidelines 40 Fed Reg 28,952 (system of records definition "limits the applicability of **some** of the provisions of the Act" – emphasis added). But see Privacy Commission Report at 503-504 (assuming that the definition limits the entire Act). Eg, in *Albright v US* 631 F 2d 915, 918-920 (DC Cir 1980), the court held that subsection (e)(7) (see text to fn 320) applies even to records not incorporated into a system of records. *Albright* involved a challenge on subsection (e)(7) grounds to an agency's maintenance of a videotape – kept in a file cabinet in an envelope that was not labelled with any individual's name – of a meeting between a personnel officer and agency employees affected by the officer's job reclassification decision. Relying on both the broad definition of "maintain" and the "special and sensitive" treatment accorded First Amendment rights, the DC Circuit held that the mere collection of a record regarding those rights could be a violation of subsection (e)(7), regardless of whether the record was contained in a system of records retrieved by an individual's name or personal identifier.

4.2.2.4 Conditions of disclosure

The Act's "guiding principle"[236] and probably the most important provision of the Act, is section 552a(b), which provides that no federal agency may disclose any record contained in a system of records by any means of communication to any person or to another agency unless:

- the individual to whom the record pertains has, before such disclosure, requested or consented to such disclosure in writing
- such disclosure falls within one of the listed exceptions[237]

Violation of this section may lead to civil liability or criminal penalties.[238]

It has frequently been held that a "disclosure" under the Privacy Act does not occur if the communication is to a person who is already aware of the information.[239] One might argue that to say that no "disclosure" occurs for previously published or public information is inconsistent with the Supreme Court's decision in *United States Department of Justice v Reporters Committee for Freedom of the Press*,[240] which held that a privacy interest can exist, under the FOIA, in publicly available – but "practically obscure" – information, such as a criminal history record.[241]

---

236 See Graham 1987 *Tex LR* 1395, 1429.

237 5 USC s 225a(b)(1)–(12). Note that besides these exceptions to the prohibition against non-consensual disclosures, agencies may also be exempted from certain provisions of the Act (see par 4.2.2.9).

238 See par 4.2.2.13.

239 See eg *Quinn v Stone* 978 F 2d 126 (3d Cir 1992); *Kline v HHS* 927 F 2d 522 (10th Cir 1991); *Hollis v US Dept of the Army* 856 F 2d 1541 (DC Cir 1988); *Reyes v Supervisor of DEA* 834 F 2d 1093 (1st Cir 1987); *Schowengerdt v Gen Dynamics Corp* 823 F 2d 1328 (9th Cir 1987). In *Hoffman v Rubin* 193 F 3d 959 (8th Cir 1999) no Privacy Act violation was found to have occurred where an agency disclosed the same information in a letter to a journalist that the plaintiff himself had previously provided to the journalist.

240 489 US 749 (1989). See par 3.2.2 above.

241 The Court of Appeals for the District of Columbia Circuit ruled that this principle does not apply to all disseminations of protected records to individuals with prior knowledge of their existence or contents in *Pilon v US Dept of Justice* 73 F 3d 1111 1117-1124 (DC Cir 1996). In *Pilon* the DC Circuit held that the Justice Department's transmission of a Privacy Act-protected record to a former employee of the agency constituted a disclosure under the Privacy Act, even though the recipient had come into contact with the

(continued...)

By requiring the prior consent of an individual before a disclosure of a record may take place, the Act enables the individual to learn of a record kept on him or her in a federal system of records[242] and thus allows the individual to exercise his or her right of access under the Act.[243]

Certain disclosures are permitted without the prior consent of the affected individuals.[244] With the exception of disclosures required by the Freedom of Information Act (FOIA), disclosures under the following exceptions are permissible, not mandatory.[245] These exceptions are:

- ❒ within the agency that maintains the record, to those who need it in their work [246]
- ❒ as required by the FOIA [247]
- ❒ for a "routine use" (which is a use for a purpose that is compatible with the purpose for which it was collected)[248]

241(...continued)
record in the course of his duties while an employee. The court's review of the Privacy Act's purposes, legislative history and integrated structure convinced it that Congress intended the term "disclose" to apply in virtually all instances to an agency's unauthorised transmission of a protected record, regardless of the recipient's prior familiarity with it (at 1124).

242 The original draft of the Senate bill required an agency to notify all individuals about whom the agency maintained personal information of that fact. However, this requirement was abandoned owing to the allegedly prohibitive cost of notification. Instead the Act relies on the initiative of citizens to seek out information about them (Bouchard *Guidebook* 75 fn 89).

243 5 USC s 552a(d).

244 The exceptions to the prohibition against non-consensual disclosure reflect a recognition of the fact that exchange of information within the government is necessary in order for it to fulfil its generally accepted functions, but unfortunately also prevent an individual from discovering the existence of records about him or her, thus negating the benefits of the prior consent requirement (see Graham 1987 *Tex LR* 1395, 1420).

245 See OMB Guidelines 40 Fed Reg at 28,953.

246 5 USC s 552a(b)(1). The "need to know" exception allows disclosure to "officers of the agency which maintains the record" and not to other agencies. Consequently it was held that the Department of Energy's Inspector-General was not authorised by this exception to disclose employees' personnel security files to the Department of Justice (*Covert v Herrington* 663 F Supp 577 (9th Cir 1987)).

247 5 USA s 225a(b)(2). The Freedom of Information Act is codified at 5 USC s 552 (see par 4.2.4).

248 5 USC s 552a(b)(3). The compatibility requirement of the routine use exemption occurs in the definition section of the Privacy Act (5 USC s 552a(a)(7)). According to Schwartz 1995 *Iowa LR* 553, 584 the principle of compatibility "requires a significant degree of convergence and a concrete relationship between the purpose for which the information was gathered and its application".

- ❒ to the Bureau of Census for activities relating to a census, survey or related activity[249]
- ❒ for use solely as a statistical record[250]
- ❒ to the National Archives[251]
- ❒ to another agency or instrumentality of government, for a criminal or civil law enforcement activity after the head of the agency had requested this in writing, specifying the law enforcement activity for which the record is sought[252]
- ❒ for compelling health or safety reasons[253]
- ❒ to Congress[254]
- ❒ to the Comptroller General in the course of the performance of the duties of the General Accounting Office[255]
- ❒ pursuant to a Court order[256]

249 5 USC s 552a(b)(4). The exception for the Bureau of Census was justified on the grounds that it is in a different position from other federal agencies, in that it is not involved in making determinations on individuals' eligibility to benefit under federal programs. Furthermore, there are other laws that apply to the Census Bureau that limit access to census records to census employees (HR Rep 93–1416 at 12).

250 5 USC s 552a(b)(5). The recipient must give adequate written assurance in advance that the record will be used solely as a statistical or research record, and that the record is to be transferred in a form that is not individually identifiable. "Statistical record" is defined as "a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual..." (5 USC s 552a(a)(6)).

251 5 USC s 552a(b)(6). It should be a record which has sufficient historical or other value to warrant its continued preservation by the United States government.

252 5 USC s 552a(b)(7).

253 5 USC s 552a(b)(8). It was thought that in a valid emergency, such as an epidemic or plane crash, it would not be feasible to obtain prior consent because it could be a matter of life and death where instant action is required (HR Rep 93–1416 at 13). This section also requires that a notification should be sent to the last known address of the individual affected by the disclosure. See eg *Schwarz v US Dept of Treasury* 131 F Supp 2d 142 (DDC 2000).

254 5 USC s 552a(b)(9). Both Houses of Congress, as well as any subcommittee thereof, are included in this section. It was argued that Congress may find it necessary to enquire into such subjects for legislative and investigative reasons (HR Rep 93–1416 at 13).

255 5 USC s 552a(b)(10).

256 5 USC s 552a(b)(11). This exception, like the routine use exception, has generated a great deal of uncertainty. Neither the Act's legislative history, nor the OMB Guidelines, shed light on its meaning. "As a general proposition, it appears that the essential point of this exception is that the Privacy Act cannot be used to block the normal course of court proceedings, including court-ordered discovery." US Dept of

(continued...)

❒ to a consumer reporting agency pursuant to the Debt Collection Act[257]

According to one commentator, these exceptions to the rule are so broad that they threaten to swallow the rule.[258]

The most controversial of these exceptions is the so-called "routine use" exception.[259] As stated previously a routine use is a use for a purpose that is compatible with the purpose for which the information was collected.[260] An example of a "compatible" routine use that frequently occurs in the law enforcement context is that law enforcement agencies routinely share law enforcement records with one another.[261]

256(...continued)
Justice *Overview of the Privacy Act*. See *Clavir v US* 84 FRD 612 (SDNY 1979);*Martin v US* 1 Cl Ct 775 (Cl Ct 1983).

257 5 USC s 552a(b)(12). The Debt Collection Act of 1982 (Pub L 97–365, 96 Stat 1749 (1982)) was enacted to facilitate the collection of debts owed to the United States. In terms of this Act the federal government may make use of private debt collection agencies, and is permitted to disclose information concerning debtors to these agencies. This Act required an amendment to the Privacy Act in 1982, namely the addition of a twelfth exception to the prohibition on disclosures. Information cannot be disclosed indiscriminately under this exception, however, since the Debt Collection Act does place limits on the disclosure process. See further Ehlke 1985 *J Mar LR* 829, 838–839; OMB Guidelines 48 Fed Reg 15,556–60.

258 This is the view of John Shattuck of the American Civil Liberties Union, quoted in Flaherty *Surveillance societies* 323.

259 5 USC s 552a(b)(3). Congress probably inserted the provision because it is difficult to enumerate all the permitted exceptions to the disclosure restrictions, and never intended this provision to become a loophole for evading the prior consent requirement. The "routine use" exemption was part of the original House Bill (HR 16373), but not of the Senate Bill (S 3418). It became part of the compromise reached to pass the Privacy Act (see par 4.2.1.5). No clear insight into Congress's intent in passing the exemption is provided by the legislative history (see Coles 1991 *Am ULR* 957, 977). The House Bill's purpose was that the routine use exemption should contribute to orderly government, by allowing federal agencies to routinely exchange information for "housekeeping measures" (Coles 1991 *Am ULR* 957, 976). See also Flaherty *Surveillance societies* 323; Simitis 1987 *U Pa LR* 707, 741; Coles 1991 *Am ULR* 957, 978. Schwartz 1995 *Iowa LR* 553, 584 argues that agencies have ignored the limitation imposed on the routine use exemption by the principle of compatibility (see fn 248).

260 5 USC s 552a(a)(7). According to Schwartz 1995 *Iowa LR* 553, 584 the principle of compatibility "requires a significant degree of convergence and a concrete relationship between the purpose for which the information was gathered and its application".

261 See OMB Guidelines 40 Fed Reg at 28,955 (a proper routine use is the "transfer by a law enforcement agency of protective intelligence information to the Secret Service").

The Privacy Act imposes two additional requirements when the routine use exception is used: (a) At the time of collecting the information from the individual, such individual must be informed about each routine use that may be made of the information[262] and (b) such routine use must also be published in the Federal Register.[263] In *Covert v Harrington*[264] the Court of Appeals for the Ninth Circuit has engrafted a third requirement onto this exception: Actual notice of the routine use under subsection (e)(3)(C) (that is, at the time of information collection from the individual).[265]

Because the routine use provision is open to wide interpretation,[266] computer matching[267] has been

---

262 5 USA s 552a(e)(3)(C).

263 5 USC s 552a(e)(4)(D). Before a new routine use can be introduced, notice of such intended new routine use must be given 30 days before publication in terms of s 552a(e)(4)(D), enabling persons to submit written data, views, or arguments (s 552a(e)(11); also see par 4.2.2.7).

264 876 F 2d 751, 754-756 (9th Cir 1989).

265 Subsequently, the Court of Appeals for the District of Columbia Circuit cited this aspect of *Covert* with approval and remanded a case for determination as to whether (e)(3)(C) notice was provided, stating that "[a]lthough the statute itself does not provide, in so many terms, that an agency's failure to provide employees with actual notice of its routine uses would prevent a disclosure from qualifying as a 'routine use', that conclusion seems implicit in the structure and purpose of the Act". See *United States Postal Serv v Nat Ass of Letter Carriers* 9 F 3d 138, 146 (DC Cir 1993).

266 Messick 1985 *Santa Clara LR* 153, 166–167 fn 62.

267 For a definition of computer or data matching, see ch 1 par 1.3. Computer or data matching usually has the admirable aim of removing fraud, waste and abuse from government programs (Flaherty *Surveillance societies* 344). However, the following arguments have been raised against computer matching:

(a) It amounts to an unreasonable search and seizure (comparable to a "fishing expedition") and thus violates the Fourth Amendment of the US Constitution.
(b) The presumption of innocence is turned into a presumption of guilt since the burden of proof is reversed.
(c) It violates the "fair information principle" that information obtained for one purpose may not be used for another purpose (see par 4.2.2.7).
(d) "Hits" (ie persons identified as being on both lists) are denied due process of the law by not being given adequate notice of their situation and adequate opportunity to contest the result.
(e) It enables the government to build up dossiers about individuals.
(f) The line between "good" and "bad" uses may become blurred.

(See Shattuck 1984 *Hastings LJ* 991; Langan 1979 *Colum JL & Soc Probs* 143, 146–147). Flaherty *Surveillance societies* 355 points out that computer matching may lead to the creation of large new information systems, in effect just as dangerous as the Central Data Bank, the idea of which was rejected in the 1960s (see par 4.2.1.2). Schwartz 1995 *Iowa LR* 553 also points out that data matching obscures the transparency of data processing.

An early federal data matching program was "Project Match", created by the Carter administration in the Department of Health, Education and Welfare (HEW) in 1977. In this case individuals on the federal

(continued...)

justified on this ground.[268] This resulted in Congress enacting the Computer Matching and Privacy Protection Act in 1988, which amended the Privacy Act.[269]

The Computer Matching and Privacy Protection Act (CMPPA) of 1988[270]

The CMPPA has limited scope. It applies to the computerised comparison of records for establishing or verifying eligibility for a federal benefit programme, or recouping payments or delinquent debts under such programmes.[271] However, matches performed for statistical, research, law enforcement, foreign counterintelligence, security screening, and tax purposes are excluded.[272] The Act requires the agencies involved to create written agreements concerning their use of matching records.[273] Citizens must be given prior notice in the Federal Register of proposed matches.[274] Agencies must provide adequate notice of a proposal to establish, or make a significant change, to an existing system of records or a

267(...continued)
payroll were compared with individuals on the "AFDC" (Aid to Families with Dependent Children) list. A "hit" was then considered to be receiving illegal benefits under the aid programme (see Langan 1979 *Colum JL & Soc Probs* 143, 144–150; Albinger 1986 *Ann Surv Am L* 625, 627–30; Flaherty *Surveillance societies* 344; Schwartz 1992 *Hastings LJ* 1321, 1352–1365). Computer matching is also used extensively by the IRS to ferret out tax evaders. In this regard, see Messick 1985 *Santa Clara LR* 153.

268 See Flaherty *Surveillance societies* 346 and the authority cited by Ehlke 1985 *J Mar LR* 829, 832 fn 28; Simitis 1987 *U Pa LR* 707, 740–741. Other "violations" of the routine use exemption include the Securities and Exchange Commission's routine disclosure of derogatory information to other agencies, and the Civil Service Commission's transmission of information on an individual's character, reputation, and personal characteristics to other agencies (see Coles 1991 *Am ULR* 957, 982; Madsen *Personal data protection* 115).

269 The Office of Management and Budget (OMB), being responsible for oversight of the Privacy Act (see par 4.2.3), monitors computer matching programs and from time to time issues guidelines to the federal agencies in this regard. However, in 1986 the Office of Technology Assessment (OTA) of the US Congress found that "the Privacy Act as presently interpreted by the courts and OMB guidelines offers little protection to individuals who are the subjects of computer matching" (see *Electronic record systems and individual privacy* 1986 at 57 quoted in Flaherty *Surveillance societies* 357 (refer to 458–459 fn 31)). For more information on the legislative history of the CMPPA, see Regan *Legislating privacy* 95–99. See also Flaherty *Surveillance societies* 356–358; Strong 1988 *Softw LJ* 391.

270 Pub L No 100–503 (1988) codified at 5 USC ss 552a(a)(8)–(13); (e)(12); (o),(p),(q),(r)&(u).

271 5 USC s 552a(a)(8)(A).

272 5 USC s 552a(a)(8)(B).

273 5 USC s 552a(o).

274 5 USC s 552a(e)(12).

matching programme. Such notice must be given to the OMB and the oversight committees in the House and Senate.[275] If adverse data on a person are uncovered, the agency cannot take steps to cut off the benefit the person receives without validating their accuracy and offering the individual an opportunity to contest the findings.[276] Compliance with the Act must be overseen by a Data Integrity Board (DIB), to be established by each agency. The DIB reports to the OMB.[277]

4.2.2.5 Account of disclosures

The wholesale disclosure of personal information under one of the listed exceptions is restrained by the requirement that the federal agencies must keep an accurate account of disclosures they make,[278] except where a disclosure is made within the agency on the "need to know" basis,[279] or made in terms of the Freedom of Information Act.[280]

The agency must keep the date, nature and purpose of each disclosure, as well as the name and address of the person or agency the disclosure was made to,[281] for either five years or the life of the record, whichever is the longer.[282] Such an account must be made available to the individual concerned at his or her request,[283] unless the disclosure was made for law-enforcement purposes.[284] Furthermore,

275 5 USC s 552a(r).

276 5 USC s 552a(p).

277 5 USC s 552a(u).

278 5 USC s 552a(c). The OMB Guidelines specifically state that an account of disclosure is required "even when such disclosure is .. with the written consent or at the request of the individual", ie not based on an exception (OMB Guidelines 40 Fed Reg 28,948, 28,955).

279 See text to fn 246.

280 5 USC s 552a(c)(1).

281 5 USC s 552a(c)(1)(A) & (B).

282 5 USC s 225a(c)(2).

283 This subsection grants individuals a right of access similar to the access right provided by subsection (d)(1)(see fn 288 and see *Standley v Dept of Justice* 835 F 2d 216, 219 (9th Cir 1987)) (the plaintiff was (continued...)

if a correction or notation is made to a record after it was disclosed, the person or agency to whom the disclosure was made must be notified about the change, if an account was made of the disclosure.[285]

The purpose of requiring agencies to keep an account of disclosures is threefold:[286]

- ❒ to enable individuals to discover to whom their records have been disclosed
- ❒ to facilitate the correction of erroneous records
- ❒ to allow individuals to force agencies to comply with the disclosure provisions of subsection 552a(b)

Evidence suggests, however, that accounts of disclosures are not frequently sought by individuals, negating the purpose of the provision.[287]

4.2.2.6 Access to and amendment of records

The Act also provides that an individual may, upon request, have **access** to a record kept on him or her. With the individual's authorisation, a person of his or her choice may accompany him or her when reviewing the record. An individual may review the record and have a copy made of it in a form comprehensible to such individual.[288]

To strengthen the access clause, the Act also provides that an individual may request an **amendment**

283(...continued)
entitled to gain access to a list, compiled by the US Attorney, of persons in the IRS to whom disclosures of grand jury materials about the plaintiff had been made); *Ray v US Dept of Justice* 558 F Supp 226 (DDC 1982)).

284 5 USC s 225a(c)(3).

285 5 USC s 552a(c)(4).

286 Bouchard *Guidebook* 75 fn 85.

287 Privacy Commission Report 525.

288 5 USC s 552a(d)(1). Should the agency refuses access, the individual has civil remedies available (see par 4.2.2.13).

to a record about the individual,[289] if he or she believes that the record is not accurate, relevant, timely or complete.[290] The agency must acknowledge receipt of such request within ten days, and must promptly either make the correction or inform the individual of its refusal to correct the record, the reason for such refusal and the procedures for review of the refusal.[291]

If the agency is requested by the individual to **review** its decision not to amend the record, such review must be done within thirty days, and a final determination made on the issue.[292] If the agency still refuses to amend the record, the individual may take the following further action:

- File a statement setting out that he or she disagrees with the agency about the accuracy of the record, in which case the agency must, in all subsequent disclosures, clearly note the disputed part of the record and provide a copy of the individual's statement of disagreement.[293]

- Ask for judicial review in a district court, in which case the court may direct the agency to amend the record as requested, or in such way as the court may direct.[294] If the individual prevails, the court may also assess reasonable attorney and litigation fees against the government.[295]

After an individual has filed a statement contesting the accuracy of a record, the agency should clearly

289 5 USC s 552a(d)(2).

290 5 USC s 552a(d)(2)(B)(i). What the Act covers, is an error of fact, not of judgment (see *Blevins v Plummer* 613 F 2d 767 (9th Cir 1980); *Rogers v US Dept of Labour* 607 F Supp 697 (9th Cir 1985)).

291 5 USC s 552a(d)(2).

292 The head of the agency may for good cause extend the thirty day period (5 USC s 552a(d)(3)).

293 5 USC s 552a(d)(3),(4).

294 5 USC s 552a(d)(g)(1) & (2). See also par 4.2.2.13 .

295 5 USC s 552a(g)(2)(B).

note the disputed part in subsequent disclosures.[296]

4.2.2.7 Agency requirements: fair information principles

The Act imposes certain requirements on every agency that maintains a system of records. These requirements amount to a statement of "fair information principles".[297]

- An agency must maintain only information about an individual that is relevant and necessary for the stated agency purpose.[298]

  This subsection is not violated as long as the maintenance of the information at issue is relevant and necessary to accomplish a legal purpose of the agency.[299] It was held that this requirement "refers to the types of information maintained and whether they are germane to the agency's statutory mission", and "does not incorporate [an] accuracy standard".[300]

- An agency must collect information directly from the subject as far as is practicable when information can result in an unfavourable decision for the individual under a federal programme.[301]

296 5 USC s 552a(d)(4). A shortcoming in this provision is the fact that it is not required of the agency to notify all persons previously informed. Consequently, information that has been disclosed before such statement was filed can be used or relied on in making decisions to the individual's disadvantage even after the statement has been filed.

297 See Flaherty *Surveillance societies* 322. Also see ch 3 par 2.2.5 and par 3.2.4; ch 4 par 4.3.4 and ch 6 par 2.2.

298 5 USC s 552a(e)(1).

299 See, eg, *Reuber v US* 829 F 2d 133 (DC Cir 1987); *Nat Fed of Fed Employees v Greenberg* 789 F Supp 430 (DDC 1992).

300 *Felsen v HHS* No CCB-95-975 *slip opinion* at 59-61 (D Md Sept 30, 1998).

301 5 USC s 552a(e)(2). The qualification "as far as practicable" enables agencies to get around this provision by saying that because of high cost it is not practicable to collect the information from the individual himself or herself. On this section, see also Kaplan & Mahoney 1997 *Fed L'yer* 38.

The leading cases under this provision are *Waters v Thornburgh*[302] and *Brune v IRS.*[303] *Waters* involved a Justice Department employee whose supervisor became aware of information that raised suspicions concerning the employee's unauthorised use of administrative leave. Without first approaching the employee for clarification, the supervisor sought and received from a state board of law examiners verification of the employee's attendance at a bar examination. In finding a violation of this provision on these facts, the court ruled that "[i]n the context of an investigation that is seeking objective, unalterable information, reasonable questions about a subject's credibility cannot relieve an agency from its responsibility to collect that information first from the subject". The DC Circuit in *Waters* distinguished its earlier decision in *Brune*, which had permitted an IRS supervisor to contact taxpayers to check on an agent's visits to them without first interviewing the agent, based upon the "special nature of the investigation in that case – possible false statements by an IRS agent" and the concomitant risk that the agent, if contacted first, could coerce the taxpayers to falsify or secrete evidence.[304]

❒ An agency must inform individuals whom it asks to supply information[305] of the authority under which the information is gathered, whether they are obliged to give information or not, the principal purposes for which the supplied information will be used, routine uses that could be made of the information and the effects on the individuals if they refrain from giving information.[306]

The OMB Guidelines note that implicit in this subsection is the notion of informed consent since an individual should be provided with sufficient information about the request for information

302 888 F 2d 870 (DC Cir 1989).

303 861 F 2d 1284 (DC Cir 1988). See further US Dept of Justice *Overview of the Privacy Act*.

304 *Waters v Thornburgh* 888 F 2d 870 (DC Cir 1989) 874.The OMB Guidelines suggest several factors to be evaluated in determining whether it is impractical to contact the subject first. See OMB Guidelines 40 Fed Reg 28,948, 28,961.

305 On the form it uses to collect the information or on a separate form which can be retained by the individuals.

306 5 USC s 552a(e)(3).

to make an informed decision on whether or not to respond. The OMB Guidelines also note that this provision is applicable to both written and oral solicitations of personal information.[307]

- An agency must publish information about its system of records in the federal register when such a system is established or revised, including information about the name and location of the system, the categories of records maintained in the system, every routine use that could be made of the information, the policies of the agency in operating the system, the name of the official responsible for the system, the procedures to follow to obtain a notice that a record is being kept on an individual, how to gain access to records, and the categories of sources of records in the system.[308]

- An agency must maintain all records which are used by the agency in making any determination about an individual, with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individual in the determination.[309]

This provision[310] sets forth the standard to which records must conform in the context of a lawsuit involving the amendment or accuracy of a record.[311] This subsection does not require that the record should be perfect. The standard is that of "reasonableness".[312] Erroneous facts,

307 OMB Guidelines 40 Fed Reg 28,948, 28,961.

308 5 USC s 552a(e)(4). Any employee of an agency that fails to comply with this requirement is guilty of a misdemeanour (see par 4.2.2.13). The Privacy Act requires two types of publication by agencies concerning the system of records in their possession: s 552a(e)(4) requires a notice regarding the existence and character of a system of records, whereas s 552a(f) requires a promulgation of the rules to facilitate individual access to each system of records (see par 4.2.2.8). The Office of the Federal Register annually compiles and publishes the agency notices and access rules (Flaherty *Surveillance societies* 337). Flaherty questions the utility of these publications, since they are unknown to and unused by the public. See further *Pippinger v Rubin* 129 F 3d 519 (10th Cir 1997).

309 5 USC s 552a(e)(5).

310 Along with subsections (e)(1) and (e)(7).

311 See 5 USC s 552a(g)(1)(A) and 5 USC s 552a(g)(1)(C) (see fn 386, 388).

312 See *Johnston v Horne* 875 F 2d 1415 (9th Cir 1989); *DeBold v Stimson* 735 F 2d 1037 (7th Cir 1984); *Edison* (continued...)

as well as opinions, evaluations and subjective judgments based entirely on erroneous facts, can be amended.[313] As a general rule, courts are reluctant to disturb opinions, judgments or evaluations in an individual's record when such judgments are based on a number of factors or when the factual predicates for a judgment or evaluation are diverse.[314] Many courts have held that pure opinions and judgments are not subject to amendment.[315] In determining what steps an agency should take in order to satisfy the accuracy standard of this subsection, the Court of Appeals for the District of Columbia Circuit took into consideration whether the information at issue was capable of being verified.[316] Furthermore, this provision's "timeliness" requirement

312(...continued)
v Dept of the Army 672 F 2d 840, 843 (11th Cir 1982). Eg, it was held that it is reasonable for an agency – without conducting its own investigation – to maintain a record concerning an unsubstantiated allegation of sexual misconduct by an ATF agent conveyed to it by the state and local authorities (*Jones v United States Dept of the Treasury* No. 82-2420 *slip opinion* at 2-3 (DDC Oct 18, 1983) *affd* 744 F 2d 878 (DC Cir 1984)). In *Graham v Hawk* 857 F Supp 38 (WD Tenn 1994), *affd* 59 F 3d 170 (6th Cir 1995) it was held that where records contain disputed hearsay and reports from informants and unnamed parties, "the records are maintained with adequate fairness if they accurately reflect the nature of the evidence" (that is, indicate that the information is a hearsay report from an unnamed informant).

313 See, eg, *Hewitt v Grabicki* 794 F 2d 1373 (9th Cir 1986); *Douglas v Farmers Home Admin* 778 F Supp 584 (DDC 1991).

314 Eg, in *White v OPM* 787 F 2d 660 (DC Cir 1986) the court ruled that where a subjective evaluation is based on a multitude of factors and there are various ways of characterising some of the underlying factual events, it is proper to retain and rely on the record. See also *Webb v Magaw* 880 F Supp 20 (DDC 1995) (the records involved were not based on a demonstrably false premise, but rather on a subjective evaluation based on a multitude of factors); *Bernson v ICC* 625 F Supp 10 (D Mass 1984) (holding that the court cannot order amendment of opinions to reflect the plaintiffs' version of the facts); *Phillips v Widnall* No 96-2099 1997 WL 176394 (10th Cir Apr 14, 1997) (holding that appellant was not entitled to court-ordered amendment, nor award of damages, concerning a record in her medical files that contained a physician's notation to the effect that the appellant was probably dependent upon a prescription medication, as such notation reflected the physician's medical conclusion, which he based upon a number of objective factors and the appellant's own complaints of neck and low back pain).

315 See, eg, *Reinbold v Evers* 187 F 3d 348 (4th Cir 1999); *Hewitt v Grabicki* 794 F 2d 1373 (9th Cir 1986); *Blevins v Plummer* 613 F 2d 767 (9th Cir 1980).

316 In *Doe v US* 821 F 2d 694 (DC Cir 1987) the court held that the inclusion in a job applicant's record of both the applicant's and the agency interviewer's conflicting versions of an interview (in which only they were present) satisfies subsection (e)(5)'s requirement of maintaining reasonably accurate records. In rejecting the argument that the agency and reviewing court must themselves make a credibility determination as to which version of the interview to believe, the DC Circuit ruled that subsections (e)(5) and (g)(1)(C) "establish as the record-keeper's polestar, 'fairness' to the individual about whom information is gathered", and that "the 'fairness' criterion does not demand a credibility determination in the **atypical** circumstances of this case"(at 699) (emphasis added). Subsequently, the DC Circuit held that in a **typical** case, where the records at issue are "not ambivalent" and the facts described therein are "susceptible of proof", the agency (continued...)

does not require that agency records contain only information that is "hot off the presses".[317]

❒ An agency must make reasonable efforts to ensure, before disseminating a record about an individual to a person other than an agency, that such records are accurate, complete, timely and relevant for agency purposes.[318]

This provision requires a reasonable effort by the agency to review records prior to their dissemination.[319]

❒ An agency may not maintain records on how an individual exercises his or her First Amendment rights, unless the keeping of such records has been authorised by the individual or statute, or is for a law enforcement activity.[320]

Assuming that the challenged record itself describes an activity protected by the First Amendment,[321] subsection (e)(7) is violated unless the maintenance of the record is (i) expressly authorised by statute,[322] or (ii) expressly authorised by the individual about whom the

316(...continued)
and reviewing court must determine accuracy as to each filed item of information (*Strang v US Arms Control & Disarmament Agency* 864 F 2d 859 (DC Cir 1989)).

317 *White v OPM* 787 F 2d 660 (DC Cir 1986) (rejecting an argument that the use of a year-old evaluation violates the Act, as it would be an unwarranted intrusion on the agency's freedom to shape employment application procedures); see also *Beckette v U S Postal Serv* No 88-802 *slip op* (ED Va July 3, 1989).

318 5 USC s 552a(e)(6). Where the records are disseminated because of a request under the FOIA, this provision does not apply (*Smith v US* 817 F 2d 86 (10th Cir 1987); see also OMB Guidelines 40 Fed Reg).

319 See *NTEU v IRS* 601 F Supp 1268 (DDC 1985).

320 5 USC s 552a(e)(7).

321 The OMB Guidelines advise agencies in determining whether a particular activity constitutes the exercise of a right guaranteed by the First Amendment to apply the broadest reasonable interpretation (40 Fed Reg 28,948, 28,965). As noted above (see fn 235), *Albright v US* 631 F 2d 915, 918–920 (DC Cir 1980) established that the record at issue need not be within a system of records to violate subsection (e)(7).

322 See eg *Abernethy v IRS* 909 F Supp 1562 (ND Ga 1995).

record is maintained,[323] or (iii) pertinent to and within the scope of an authorised law enforcement activity.[324]

- An agency must make reasonable efforts to serve notice on an individual that information on him or her was given out under a compulsory legal process, when such process becomes part of a public record.[325]

  This provision becomes applicable when a subsection (b)(11) court order disclosure occurs.[326]

- An agency must establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.[327]

- An agency must establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to guard against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment,

---

323 See *Abernethy v IRS* 909 F Supp 1562, 1570 (ND Ga 1995) ("Plaintiff authorized the maintenance of the documents at issue by submitting copies to various components of the Defendant IRS"). See also OMB Guidelines 40 Fed Reg at 28,965 ("volunteered" information is properly maintained).

324 See *Patterson v FBI* 893 F 2d 595 (3d Cir 1990). The purpose of the exception to this subsection is not to dilute First Amendment rights, but to make certain that political and religious activities are not used as a cover for illegal or subversive activities (*Clarkson v IRS* 678 F 2d 1368 (11th Cir 1982)). There should be a direct *nexus* between the records and the authorised criminal, civil or administrative law enforcement activity (*Jabara v Webster* 691 F 2d 272 (6th Cir 1982)).

325 5 USC s 552a(e)(8).

326 See fn 256. See eg *Moore v US Postal Serv* 609 F Supp 681(EDNY 1985); see also OMB Guidelines 40 Fed Reg 28,948, 28,965.

327 5 USC s 552a(e)(9). For a discussion of this provision, see OMB Guidelines 40 Fed Reg 28,948, 28,965.

inconvenience or unfairness to an individual on whom information is maintained.[328]

This provision may come into play when documents are "leaked".[329]

- An agency must, at least thirty days before the publication of a routine use in the Federal Register, publish notice of a new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views or arguments to the agency.[330]

- An agency must at least thirty days before conducting a matching program with a non-federal agency, publish in the Federal Register notice of the establishment or revision of the matching program.[331]

An employee of an agency that fails to comply with these requirements is guilty of a misdemeanour[332] and such failure to comply may also result in a civil action.[333]

4.2.2.8 Agency rules

To carry out the provisions of the Act, an agency must promulgate rules which

- establish procedures whereby individuals can be notified in response to their requests if a

328 5 USC s 552a(e)(10).

329 See eg *Pilon v US Dept of Justice* 796 F Supp 7 (DDC 1992) (holding that because subsection (e)(10) is more specific than subsection (b), it prevails with regard to allegedly inadequate safeguards that resulted in disclosure).

330 5 USC s 552a(e)(11). For a discussion of this provision, see OMB Guidelines 40 Fed Reg 28,948, 28,966.

331 5 USC s 552a(e)(12). This section was inserted by the CMPPA of 1988 (see fn 270).

332 See 5 USC s 552a(i)(2) and par 4.2.2.13.

333 5 USC s 552a(g). See further par 4.2.2.13.

system of records named by the individuals contains records pertaining to them

- define reasonable times, places and requirements for identifying individuals who request their records or information pertaining to them, to give such individuals access to information in such records, and to review requests to amend records

- establish procedures for the disclosure to individuals upon their request of their records or information pertaining to them, including special procedures, if deemed necessary, for the disclosure of medical records, including psychological records, pertaining to the individuals[334]

- establish procedures for reviewing requests from individuals concerning the amendment of records or information pertaining to them, for making a determination on the requests, for an appeal within the agency against an initial adverse agency determination, and for whatever additional means may be necessary to enable each individual to exercise fully his or her rights

- establish fees to be charged, if any, to individuals for making copies of their records, excluding the cost of a search for and review of the records[335]

Such rules must be compiled and published biennially by the Office of the Federal Register in a form available to the public at low cost.[336]

---

334 See *Benavides v US Bureau of Prisons* 995 F 2d 269 (DC Cir 1993). This court held that such rules may not result in the applicant not being allowed to see the medical files. The Privacy Act does not require direct disclosure of medical records to the individual. Recognising the "potential harm that could result from unfettered access to medical and psychological records", the court provided that "as long as agencies guarantee the ultimate disclosure of the medical records to the requesting individual... they should have freedom to craft special procedures to limit the potential harm".

335 Unlike under the FOIA, search and review costs are never chargeable under the Privacy Act. See OMB Guidelines 40 Fed Reg 28,948, 28,968.

336 5 USC s 552a(f). For a discussion of this provision, see OMB Guidelines 40 Fed Reg 28,948, 28,967. See also fn 308.

4.2.2.9 Exemptions

Besides the twelve listed exceptions to the prohibition against non-consensual disclosure,[337] the Act also contains one special, two specific and seven general exemptions. If an agency wants its system of records to be exempted in terms of the two general or seven specific exemptions, the head of the agency must claim such exemption by promulgating rules to that effect. The reason for exempting the system of records must be given in the rules.[338]

a One special exemption

There is one special exemption in the Act which is sometimes overlooked as it is not located with the other exemptions. It is an exemption from only the access provision of the Privacy Act, and it provides that "nothing in this [Act] shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding".[339]

This exemption provision reflects Congress's intent to exclude civil litigation files from access.[340] This provision shields information that is compiled in anticipation of court proceedings or quasi-judicial administrative hearings.[341] Unlike all the other Privacy Act exemptions discussed below, however, this provision is entirely "self-executing", inasmuch as it does not require an implementing regulation in order

337 See par 4.2.2.4.

338 5 USC s 552a(j),(k); *Ryan v Dept of Justice* 595 F 2d 954 (4th Cir 1979). The scope of the Act is severely limited by the general and specific exemptions. An agency may decide for itself which system of records it wants to exempt. Although the existence of an exempt system must be disclosed, the agency need not disclose the details of an exempt system, nor does it have to grant an individual access to his file within the system. According to Petrocelli *Low profile* 216, out of 6424 record systems that were in existence in 1977, 898 have been declared exempt by the various agencies involved, and these are usually the ones an individual would most like to see.

339 5 USC s 552a(d)(5).

340 See 120 Cong Rec 36,959-60 (1974). Also see *Martin v Office of Special Counsel* 819 F 2d 1181 (DC Cir 1987); *Hernandez v Alexander* 671 F 2d 402 (10th Cir 1982); *Blazy v Tenet* 979 F Supp 10 (DDC 1997).

341 See eg, *Martin v Office of Special Counsel* 819 F 2d 1181 (DC Cir 1987); *Nazimuddin v IRS* No 99-2476 2001 WL 112274 (SD Tex Jan 10, 2001); see also OMB Guidelines 40 Fed Reg 28,948, 28,960 ("civil proceeding" -term intended to cover "quasi-judicial and preliminary judicial steps").

to be effective.[342]

b Two general exemptions

A system of records that is maintained by the CIA[343] or a criminal law enforcement agency[344] may be generally exempted from some provisions of the Act. In the case of a criminal law enforcement agency, the system of records must consist of the following:

- information compiled for the purposes of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status

- information compiled for the purposes of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual

- reports that can be identified with an individual, compiled during the process of enforcement of the criminal laws, in other words, from the time of arrest or indictment right through to the release from supervision[345]

342 *Mervin v Bonfanti* 410 F Supp 1205 (DDC. 1976).

343 5 USC s 552a(j)(1). See, eg, *Alford v CIA* 610 F 2d 348 (5th Cir 1980), *Blazy v Tenet* 979 F Supp 10 (DDC 1997).

344 Including police efforts to prevent, control or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities (5 USC s 552a(j)(2)). This subsection's threshold requirement is that the system of records be maintained by "an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws". This requirement is usually met by such obvious law enforcement components as the FBI.

345 5 USC s 552a(j)(2).

However, the above-mentioned systems may **not** be exempted[346] from the requirement that the conditions of disclosures be obeyed;[347] that an account be made and kept of disclosures;[348] that notice must be given in the Federal Register of the existence and character of a system of records;[349] that reasonable efforts must be made to ensure that records are accurate, timely, and relevant for agency purposes before the records are disseminated;[350] that no records be kept on First Amendment activities;[351] that rules of conduct be established for persons handling personal information;[352] that safeguards be establish to ensure the security of records;[353] that notice be given of new intended uses of the information;[354] that the provisions regarding criminal penalties be applied.[355]

Bouchard points out that in spite of the above-mentioned exclusions from the general exemption provision, in practise the CIA and law enforcement agencies have immunity from almost every significant restriction in the Act.[356] For example, although an exemption is not allowed from the notice and consent provisions,[357] a law enforcement agency of any governmental unit can obtain personal records without either notice to, or consent by, the subject, if the agency head requests the records in

346 5 USC s 225a(j).

347 Ie 5 USC s 552a(b). See par 4.2.2.4.

348 Ie 5 USC s 552a(c)(1),(2). See par 4.2.2.5.

349 Ie 5 USC s 552a(e)(4)(A)–(F). See par 4.2.2.7. They may be exempted from 5 USC s 552a(e)(4)(G)–(H), ie the notice requirements regarding agency procedures.

350 Ie 5 USC s 552a(e)(6). See par 4.2.2.7.

351 Ie 5 USC s 552a(e)(7). See par 4.2.2.7.

352 Ie 5 USC s 552a(e)(9). See par 4.2.2.7.

353 Ie 5 USC s 552a(e)(10). See par 4.2.2.7.

354 Ie 5 USC s 552a(e)(11). See par 4.2.2.7.

355 Ie 5 USC s 552a(i). See par 4.2.2.13.

356 Bouchard *Guidebook* 55–56.

357 Ie, 5 USC s 552a(b).

writing and certifies that they will be used for law enforcement purposes.[358] Similarly, although the law enforcement agencies are not exempt from the provisions requiring an accounting of disclosures,[359] the agencies are in any event, by virtue of other subsections of the Act,[360] not obliged to make an account of disclosures for law enforcement purposes available to a subject. Also, although law enforcement agencies ostensibly cannot escape the ban on the collection of information about the exercise of First Amendment rights, such collection is permitted for law enforcement activities by the very section prohibiting such collection by other agencies.[361]

c Seven specific exemptions

An agency whose system of records has a certain content or purpose may be exempted from specific provisions of the Act, upon promulgation of rules in this regard by the head of the agency.[362]

The system may be exempted if the records are:

- ❒ classified information[363]
- ❒ investigatory material compiled for law enforcement purposes that is not generally exempted[364]

---

358 5 USC s 552a(b)(7). See par 4.2.2.4.

359 5 USC s 552a(c)(1)&(2).

360 5 USC s 225a(c)(3) read with 5 USC s 552a(b)(7). See also par 4.2.2.4.

361 5 USC s 552a(e)(7). See par 4.2.2.7.

362 5 USC s 552a(k). As mentioned above (see par 4.2.2.9), the rules must state what the reasons are why the system of records is to be exempted from a provision of the Act.

363 5 USC s 552a(k)(1). Classified information is dealt with in 5 USC s 552(b)(1).This subsection simply incorporates an FOIA exemption 1, 5 USC s 552(b)(1) (see *Keenan v Dept of Justice* No 94-1909 *slip op* at 2 n2, 7–9 (DDC 1997); *Blazy v Tenet* 979 F Supp 10 (DDC 1997).

364 5 USC s 552a(k)(2). This exemption covers: (i) material compiled for criminal investigative law enforcement purposes, by nonprincipal function criminal law enforcement entities; and (ii) material compiled for other investigative law enforcement purposes, by any agency. The material must be compiled for some investigative "law enforcement" purpose, such as a civil investigation or a criminal investigation by a nonprincipal function criminal law enforcement agency. See eg *Gowan v US Dept of the Air Force* 148 F 3d 1182 (10th Cir 1998). In terms of a proviso to this subsection an individual must be given access to the exempted information if the individual is, as a result of the maintenance of the records, denied any right,

(continued...)

- ❒ maintained in connection with providing protective services to the President or other individual[365]
- ❒ required by statute to be maintained and used solely as statistical records[366]
- ❒ investigatory material compiled solely for determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts or access to classified information, but only to the extent necessary to keep the source of such information confidential as promised[367]
- ❒ test or examination material used solely to determine individual qualifications for appointment or promotion in the federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process[368]
- ❒ evaluation material used to determine potential for promotion in the armed forces, but only to the extent necessary to keep the source of the information confidential as promised[369]

The specific provisions from which a covered system may be exempted, are:

- ❒ the requirement that an account that is kept of disclosures be made available to the individual

---

364(...continued)
privilege, or benefit to which he or she is otherwise entitled under federal law, or for which he or she would otherwise be eligible. The source of the information may not be revealed, however, if confidentiality was promised. See *Viotti v US Air Force* 902 F Supp 1331 (D Colo 1995).

365 5 USC s 552a(k)(3).This exemption is applicable to certain Secret Service record systems. See further OMB Guidelines 40 Fed Reg 28,948, 28,973.

366 5 USC s 552a(k)(4). See OMB Guidelines 40 Fed Reg 28,948, 28,973.

367 5 USC s 552a(k)(5).This exemption is generally applicable to source-identifying material in background employment and personnel-type investigative files. This subsection – known as the "Erlenborn Amendment" – was among the most hotly debated of any the Act's provisions because it provides for absolute protection to those who qualify as confidential sources, regardless of the adverse effect that the material they provide may have on an individual. See 120 Cong Rec 36,655-58 (1974). However, this subsection is a narrow exemption in two respects. First, it requires an express promise of confidentiality for source material acquired after the effective date of the Privacy Act (September 27, 1975) (see *Viotti v US Air Force* 902 F Supp 1331 (D Colo 1995)); second, this subsection protects only source-identifying material, not all source-supplied material.

368 5 USC s 552a(k)(6). It should be noted that material exempt from Privacy Act access under this subsection is also typically exempt from FOIA access. See further OMB Guidelines 40 Fed Reg 28,948, 28,974.

369 5 USC s 552a(k)(7).

concerned at his or her request[370]

- ❒ the access and amendment requirement[371]
- ❒ the requirement that the notice published in the Federal Register as to the existence of the system of records include information about agency procedures and the categories of sources of records in the system[372]
- ❒ the requirement that the agency establish rules to carry out the provisions of the Act[373]

Bouchard points out that virtually every law enforcement record qualifies for an exemption under either the general exemption provision or the provision for specific exemptions.[374]

4.2.2.10 Archival records

An agency record, pertaining to an identifiable individual, which is transferred to the Archivist of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States government, is exempted from most of the provisions of the Act.[375] However, it is not exempted from the provisions requiring an agency to publish a notice of the existence and character of the system of records and the requirement that rules of conduct should be established

370 Ie 5 USC s 552a(c)(3). See par 4.2.2.5. But note that disclosures made pursuant to 5 USC s 552a(b)(7), ie to another agency for law enforcement purposes, are in any case always excluded from 5 USC s 552a(c)(3).

371 Ie 5 USC s 552a(d). See par 4.2.2.6.

372 Ie 5 USC s 552a(e)(4)(G),(H),(I). See par 4.2.2.7.

373 Ie 5 USC s 552a(f). See par 4.2.2.8.

374 See Bouchard *Guidebook* 56. An analysis of these two provisions shows that as far as law enforcement agencies are concerned, there are only two significant distinctions between them: (a) while an agency relying on subsection (k)(2) must ordinarily provide damaging information to an individual adversely affected by its use, subsection (j) has no such requirement; (b) only subsection (j) exempts agencies from the civil remedies provision. Bouchard *Guidebook* 57 finds it disturbing that Congress apparently believes that legitimate law enforcement needs should always take priority over individual privacy. The commentator argues that the only legitimate grounds for exempting law enforcement records are (a) the need to protect the secrecy of pending investigation (b) the safety of undercover agents; and (c) the secrecy of certain investigative techniques.

375 5 USC s 552a(l).

for people involved in maintaining the information.[376]

4.2.2.11 Mailing lists

An agency may not sell or rent an individual's name and address as part of a mailing list, unless specifically authorised by law.[377]

4.2.2.12 Social security numbers

The Privacy Act section 7[378] makes it unlawful for a federal, state or local agency[379] to deny an individual any right, benefit or privilege provided by law because of the individual's refusal to disclose his or her social security account number.[380] However, disclosures required by federal statute or made to an agency maintaining a system of records dating from before 1975 under regulations or statutes then in force are exempted.[381] An agency that requests a social security number must inform the individual whether disclosure is voluntary or mandatory, under what authority it is solicited and what uses will be made of it.[382]

---

376 Ie 5 USC s 552a(e)(4)(A)–(G) and (e)(9).

377 5 USC s 552a(n).

378 Public Law 93–579. S 7 has not been codified as part of 5 USC s 552a.

379 As mentioned previously, this section is an exception to the rule that the Privacy Act only applies to federal agencies (see fn 215). However, according to Komuves 1998 *J Mar J Computer & Inf L* 529, 554 (esp fn 138) there is authority to suggest that an action against a state agency will be barred from suit under the 11th Amendment. The US Constitution Amendment 11 provides:

> The judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by citizens of another state, or by citizens or subjects of any foreign state.

380 S 7 does not explicitly provide remedies for its violation, but courts have issued declaratory and injunctive relief (Komuves 1998 *J Mar J Computer & Inf L* 529, 553). See the article by Komuves for detail on court decisions under s 7.

381 Pub L No 93–579, s 7(a)(2), 88 Stat 1897 (1974).

382 Pub L No 93–579, s 7(b), 88 Stat 1897 (1974). See *Brookens v US* 627 F 2d 494 (DC Cir 1980).

4.2.2.13 Remedies and sanctions

a Civil remedies

Under the Privacy Act, an individual may bring a civil action[383] in a district court against an agency[384] on the following grounds:[385]

- refusal by a reviewing officer to amend the individual's record after a review of the initial refusal by the agency, or failure to carry out such a review in conformity with the requirements of the Act[386]

- refusal of the individual's request to have access to his or her record, to review it or to have a copy made of it[387]

- failure of an agency to maintain an accurate, relevant, timely and complete record on an individual to the extent necessary to assure fairness in any determination relating to the qualifications, character, rights or opportunities of, or benefits to the individual that may be

383 The action must be brought within two years from the date on which the cause of action arises, or within two years after discovery by the individual that an agency has materially and wilfully misrepresented any information required to establish the liability of the agency (5 USC s 225a(g)(5)).

384 A civil action must be brought against the agency, not against the individual government officials (see, eg, *Nichols v Block* 656 F Supp 1436 (D Mont 1987); *Stephens v Tennessee Valley Authority* 754 F Supp 579 (ED Tenn 1990); *Krebs v Rutgers* 797 F Supp 1246 (DNJ 1992)).

385 Several courts have stated that the remedies provided for by the Privacy Act are exclusive, in that a violation of the Act does not provide any relief in the course of a federal criminal prosecution (see, eg, *US v Bressler* 772 F 2d 287 (7th Cir 1985); *US v Bell* 734 F 2d 1315 (8th Cir 1984)). However, it has also been held that a court may order equitable relief in the form of the expungement of records either in an action under the Privacy Act or in a direct action under the Constitution (see eg *Doe v US Air Force* 812 F 2d 738, 741 (DC Cir 1987); *Smith v Nixon* 807 F 2d 197, 204 (DC Cir 1986)).

386 5 USC s 552a(g)(1)(A). The review procedures are set out in s 225a(d)(3). See par 4.2.2.6.

387 5 USC s 552a(g)(1)(B). The access, review and copy provisions are in 5 USC s 552a(d)(1). Again, all administrative remedies must have been exhausted before an access lawsuit can be brought (see, eg, *Vaughn v Danzig* 18 Fed Appx 122 (4th Cir 2001) (*per curiam*); *Taylor v US Treasury Dept* 127 F 3d 470 (5th Cir 1997); *Phillips v Widnall* No 96-2099 1997 WL 176394 (10th Cir Apr 14, 1997); *Haase v Sessions* 893 F 2d 370 (DC Cir 1990)).

made based on such record, so that as a consequence a determination is made that does not favour the individual[388]

- failure of an agency to comply with any other provision of the Act, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual[389]

The Privacy Act provides for four separate and distinct civil causes of action, namely an amendment lawsuit,[390] an access lawsuit,[391] an accuracy lawsuit[392] and a lawsuit for other damages.[393] Amendment lawsuits and access lawsuits provide for injunctive relief (that is, the court may order the agency to amend the individual's record as requested, or as the court may direct, or the court may order the production of records improperly withheld),[394] and accuracy lawsuits and lawsuits for other damages provide for compensatory relief in the form of monetary damages (that is, the court may award actual damages (of no less than one thousand dollars) sustained by the individual because of the agency's action), but only if the court decides that the agency acted intentionally or wilfully.[395]

This means that in order to bring a damages action in an accuracy lawsuit, an individual has the burden

388 5 USC s 552a(g)(1)(C).

389 5 USC s 552a(g)(1)(D).

390 5 USC s 552a(g)(1)(A). Before a civil action for amendment of records can be instituted, it is a prerequisite that all administrative remedies must have been exhausted, ie through the pursuit of an amendment request to the agency and a request for administrative review. The exhaustion principle is well established in the Privacy Act case law. See, eg, *Quinn v Stone* 978 F 2d 126, 137–138 (3d Cir 1992); *Hill v US Air Force* 795 F 2d 1067, 1069 (DC Cir 1986).

391 5 USC s 552a(g)(1)(B).

392 5 USC s 552a(g)(1)(C).

393 5 USC s 552a(g)(1)(D).

394 5 USC S 552a(g)(2)(A); 5 USC s 552a(g)(3)(A).

395 5 USC s 552a(g)(4). See *Daniels v St Louis VA Regional Office* 561 F Supp 250 (DC Mo 1983); *Pilon v US Dept of Justice* 796 F Supp 7 (DDC 1992). Note that damages are not recoverable in an access case (*Thurston v US* 810 F 2d 438 (4th Cir 1987); *Haddon v Freeh* 31 F Supp 2d 16 (DDC 1998); *Quinn v HHS* 838 F Supp 70 (WDNY 1993)).

of proving that (i) a defective record (ii) proximately caused (iii) an adverse determination concerning him,[396] and in addition, the agency must be found to have acted in an "intentional or willful" manner. The words "intentional" and "willful" are "terms of art".[397] The Act's legislative history indicates that this unique standard is "[o]n a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct", and that it "is viewed as only somewhat greater than gross negligence".[398]

In amendment lawsuits and access lawsuits, the court may award the complainant reasonable attorney fees and other litigation costs reasonably incurred, if the complainant has substantially prevailed.[399] In damages lawsuits, the costs of the action together with reasonable attorney fees as determined by the court are recoverable by the prevailing plaintiff.[400]

Commentators argue that the Act has a weak remedial scheme, making enforcement by individuals difficult.[401] For example, individuals cannot enjoin an agency to disclose information.[402] The only

396 See, eg, *Deters v US Parole Comm* 85 F 3d 655 (DC Cir 1996); *Rose v US* 905 F 2d 1257 (9th Cir 1990); *Johnston v Horne* 875 F 2d 1415 (9th Cir 1989); *White v OPM* 840 F 2d 85 (DC Cir 1988).

397 *White v OPM* 840 F 2d 85 (DC Cir 1988).

398 120 Cong Rec 40,406 (1974). While not requiring premeditated malice (see *Parks v IRS* 618 F 2d 677 683 (10th Cir 1980), the voluminous case law construing this standard makes clear that it is a formidable barrier for a plaintiff seeking damages (US Dept of Justice *Overview of the Privacy Act*).

399 5 USC s 552a(g)(2)(B) and 5 USC s 552a(g)(3)(B). The purpose of this sub-section is not to reward successful litigants, but to ensure that the costs of litigation would not be a barrier to an average individual seeking to ascertain the accuracy of information maintained on him or her by the government (*Anderson v US Dept of Treasury* 648 F 2d 1 (DC Cir 1979)).

400 5 USC s 552a(g)(4)(B). Such an award is not discretionary. See OMB Guidelines 40 Fed Reg 28,948 28,970.

401 Ehlke 1985 *J Mar LR* 829. This author points out that litigation under the Act is a rare occurrence, as illustrated by the fact that during the first ten years of the Act's existence the Supreme Court did not decide any case under it. He blames the Act's "inherent definitional limitations, extensive exceptions and exemptions, and... generally ineffective remedial scheme... features that are not hospitable to obtaining effective relief for violations of the Act..." (841). See also Flaherty*Surveillance societies* 315; Schwartz 1995 *Iowa LR* 553 596.

402 It was held that the Act only authorises a court to give an injunction so that an individual can gain access to a record improperly withheld by the agency and can amend the record; no broad injunctive relief was to be implied under the Act (*Edison v Dept of the Army* 672 F 2d 840 (11th Cir 1982); *Parks v IRS* 618 F 2d 677 (10th Cir 1980); *Wanbun-Inini v Sessions* 900 F 2d 1234 (8th Cir1990)). Also see Schwartz 1995 *Iowa LR* 553, 596.

remedy is actual damages after the fact, provided that the individual can prove that the agency acted wilfully or intentionally,[403] and that the agency action affected him her adversely.[404] Since it may not always be possible to prove actual damages, this may mean that individuals may not get any compensation, although they might have proved that the agency acted wilfully or intentionally. It is uncertain whether actual damages include only out-of-pocket expenses, or whether physical and emotional damages are also recoverable.[405]

The fact that individuals have to prove intent or wilfulness in order to succeed in a civil action is also unsatisfactory. Negligence on the part of the agency can have just as severe consequences for individuals as intentional digressions.[406]

b Criminal penalties

The Act provides for criminal penalties (not exceeding five thousand dollars) to officers or employees of agencies in two instances:

- ❒ if they have wilfully disclosed agency records containing individually identifiable information,

403 5 USC s 552a(g)(4). See also *Clarkson v IRS* 678 F 2d 1368 (11th Cir 1982).

404 5 USC s 552a(g)(1)(C),(D). Emotional trauma alone is sufficient to qualify as an "adverse effect", according to *Albright v US* 732 F 2d 181 (DC Cir 1984). In order to be successful the plaintiff also has to prove a causal link between the agency's wilful action, and the actual damages sustained by her (*Moleiro v FBI* 749 F 2d 815 (DC Cir 1984)).

405 In *Johnson v Dept of the Treasury* 700 F 2d 971 (5th Cir 1983) it was held that "actual damages" include damages for physical and mental injury for which there is evidence in the record, but in *Fitzpatrick v IRS* 665 F 2d 327 (11th Cir 1982) the court decided that actual damages do not extend to mental injuries, loss of reputation, embarrassment or other unquantifiable injuries. Since the plaintiff in that case did not introduce evidence of expenses for psychiatric care or other pecuniary loss, he could not recover beyond the statutory minimum damages of a $1,000.

406 See, however, *South v FBI* 508 F Supp 1104 (ND Ill 1981) where it was held that "intentional or wilful" should, in the light of the legislative history of the Act, be given a broader scope than the common definition would imply. In some cases the courts seem to apply a "gross negligence" standard (*Chapman v NASA(II)* 736 F 2d 238 (5th Cir 1984), whereas in other cases a "greater than gross negligence" standard is applied (*Moskiewicz v US Dept of Agriculture* 791 F 2d 561 (7th Cir 1986); *Johnston v Horne* 875 F 2d 1415 (9th Cir 1989).

while knowing that such disclosure is prohibited by the Act[407]

- ❒ if they have maintained a system of records without meeting the notice requirements of the Act[408]

Any person who knowingly and wilfully requests or obtains a record concerning an individual from an agency under false pretences is also guilty of a misdemeanour and can be fined not more than five thousand dollars.[409]

4.2.2.14 Report on new systems

Each agency that proposes to establish or make a significant change in a system of records[410] must give adequate advance notice of such proposal to the House of Representatives Committee on Government Operations, the Senate Committee on Governmental Affairs and the Office of Management and Budget.[411] The purpose of this is to enable an evaluation of the probable or potential effect of such proposals on the individual's privacy rights.[412]

---

407 5 USC s 552a(i)(1).

408 5 USC s 552a(i)(2).

409 5 USC s 552a(i)(3). There have been at least two criminal prosecutions for unlawful disclosure of records protected under the Privacy Act. See *US v Trabert* 978 F Supp 1368 (D Colo 1997) (defendant found not guilty; prosecution did not prove "beyond a reasonable doubt that defendant 'willfully disclosed' protected material"; evidence presented constituted, at best, gross negligence and thus was insufficient for purposes of prosecution under the Privacy Act); *US v Gonzales* No 76-132 (MD La Dec 21, 1976) (guilty plea entered).

410 New matching programs or changes to matching programs should also be reported. The reference to matching programs has been inserted by the CMPPA (see fn 270).

411 These institutions are all involved in the oversight of the Act (see par 4.2.3).

412 5 USC s 552a(r).

4.2.3 Implementation and oversight of Privacy Act

There is no data protection authority in the true sense of the word to oversee the implementation of the Privacy Act.[413] Oversight takes place on different levels, namely by the head of the agency, the Office of Management and Budget (OMB), the US President, Congress and the courts.

4.2.3.1 Oversight by head of agency

The head of each federal agency is ultimately responsible for implementing the Act.[414] The premise is that each agency should handle its own information decisions and its own privacy issues.[415] Outsiders can monitor information handling practices by reviewing the reports of new and substantially altered information systems that agencies are required to submit to Congress and the OMB.[416] The Act does not prescribe how agencies should go about implementing supervision of compliance with the Privacy Act.[417] Most agencies supervise implementation of the Act through a Privacy Officer, except the Department of Defense, which has established a Defense Privacy Board.[418] However, as agencies have

413 The major dispute when enacting the Privacy Act was how the Act was to be implemented. The method chosen in the end is described by Bennett *Regulating privacy* 170 as "voluntary compliance and self-help". In other words, the agencies must themselves comply with the Act and an individual has to enforce his or her rights under the Act through the courts. See also Bennett *Regulating privacy* 172–173.

414 Flaherty *Surveillance societies* 315; Bennett *Regulating privacy* 171.

415 See fn 333.

416 See par 4.2.2.7.

417 According to a circular (Circular A–130 *Management of Federal Information Resources* 52739 – quoted in Flaherty *Surveillance societies* 334) issued by the OMB, the head of each agency must:
- annually review agency record keeping and disposal policies and practices
- every three years review the routine use disclosures associated with each system of records
- every three years review the exemption rules promulgated for each system of records
- every year review each matching program in which the agency has participated
- review annually each system of records notice to ensure that it is accurate

Flaherty *Surveillance societies* 334 remarks that if agencies complied faithfully with these requirements, the implementation of the Privacy Act would take a quantum leap forward.

418 Flaherty *Surveillance societies* 318; Bennett *Regulating privacy* 173. The Privacy Officers are usually not highly placed in an agency and also have other responsibilities. The Department of Defense's Privacy Board functions effectively, however. It consists of representation at senior level and has a (small) (continued...)

found the Act to be an annoyance, the Privacy Officers more often than not have to spend their time guiding an agency through the Privacy Act so that they can attain their goals, rather than serving as a voice for privacy.[419]

4.2.3.2 Oversight by Office of Management and Budget

The Privacy Act entrusts the oversight of its implementation to the Office of Management and Budget,[420] which is part of the executive office of the President.[421] In 1980, this responsibility was delegated to a newly created office, the Office of Information and Regulatory Affairs (OIRA).[422] In terms of the Act, the functions of the OMB (now the OIRA) are twofold, namely to:

- develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for agencies in implementing the provisions of the Act[423]

- provide continuing assistance to and oversight of the implementation of the Act by the agencies[424]

418(...continued)
permanent staff (Bennett *Regulating privacy* 173; Flaherty *Surveillance societies* 318).

419 Plesser *Oversight of the Privacy Act* 227 (quoted in Flaherty *Surveillance societies* 318).

420 Bennett *Regulating privacy* 175–177, who views the Privacy Act's regulatory choice as one of "voluntary compliance and self-help" (see fn 413), indicates that supervision by the OMB and also by Congress (see par 4.2.3.4) means that the Act does reveal aspects of "institutional control".

421 5 USC s 552a(v). As seen (par 4.2.1.5), this was part of the compromise reached at the end of the 1974 Congressional session, in order to pass the Privacy Act in that session.

422 This was done in s 3 of Pub L 96–511, 94 Stat 2825, (the "Paperwork Reduction Act"). The Paperwork Reduction Act of 1980 centralised the information functions of the OMB in the OIRA, and according to Gellman 1993 *Softw L J* 199, 222 slightly broadened the privacy role of the OMB, since its privacy functions were defined as including developing and implementing policies on information disclosure and confidentiality, providing agencies with advice about information security, and monitoring compliance with the Privacy Act.

423 5 USC s 552a(v)(1).

424 5 USC s 552a(v)(2).

No clarification is given of the phrases "develop guidelines and regulations" and "provide continuing assistance and oversight" and, given the legislative history of the Act, congressional intent regarding the functions of the OMB is obscure.[425] In practice, the OMB (subsequently the OIRA) has developed guidelines on the implementation of the Privacy Act (in 1975), as well as other policy guidelines.[426] Officers of the OIRA are also responsible for checking the advance notices that agencies must supply about proposed new or altered systems of records, and they scrutinise agencies' proposed disclosures of personal information as a routine practice.[427] It is also a function of the OIRA to compile the biennial report of the President, after receiving reports from the agencies.[428]

When evaluating the effectiveness of the regulatory scheme that is used to implement data protection, it is also important to take note of what the oversight body does **not** do. In brief, the OMB does not carry out inspections, audits, investigations, or handle complaints, neither is it involved in shaping new laws that may affect privacy.[429]

---

425 Bennett *Regulating privacy* 176.

426 The vast majority of OMB's Privacy Act Guidelines are published at 40 Fed Reg 28,948-78 (1975). However, these original guidelines have been supplemented in particular subject areas over the years. See 40 Fed Reg 56,741-43 (1975); 48 Fed Reg 15,556-60 (1983); 52 Fed Reg 12,990-93 (1987); 54 Fed Reg 25818-29 (1989); 56 Fed Reg 18,599-601 (proposed Apr 23, 1991); 61 Fed Reg 6428, 6435-39 (1996). See US Dept of Justice *Overview of the Privacy Act*. According to Flaherty *Surveillance societies* 329, these guidelines are not binding, but nevertheless have a strong influence on agencies, since the OMB controls the federal purse strings. It has been held that as a general rule, the OMB Guidelines are entitled to the deference usually accorded to the interpretations of the agency that has been charged with the administration of a statute. See *Quinn v Stone* 978 F 2d 126, 133 (3d Cir 1992); *Baker v Dept of the Navy* 814 F 2d 1381, 1383 (9th Cir 1987); *Albright v US* 631 F 2d 915, 919 n 5 (DC Cir 1980).

427 See par 4.2.2.7. The effectiveness of this oversight function is undermined by the fact that the OMB has no way of knowing whether these notices are in fact supplied, and can only try to persuade agencies on the issue of routine uses, since the final power of decision rests with the agency (Flaherty *Surveillance societies* 332).

428 According to Flaherty *Surveillance societies* 330 this report is usually several years late.

429 These are very important functions of a "proper" data protection authority (see Flaherty *Surveillance societies* 333, 341 and compare the functions of the British Data Protection Commissioner (see ch 4 par 4.3.9.1) and the Dutch College Bescherming Persoonsgegevens (see ch 5 par 4.3.11.1). Commentators are all critical of the passive role that the OMB has played in overseeing the Act (see Bennett *Regulating privacy* 176; Flaherty *Surveillance societies* 333; Gellman 1993 *Softw LJ* 199, 222–226). Flaherty *Surveillance societies* 326 argues that the OMB could successfully implement data protection if it had the political will to do so. (As the OMB is part of the Executive Office of the President, the relevant political will is of course that of the President.)

4.2.3.3 Oversight by President

The President of the US must biennially[430] submit a report to Congress and the House of Representatives which describes the actions of the Director of the OMB as they relate to the Privacy Act during the preceding two years, describes how individuals have exercised their rights of access and amendment under the Act during the two years, identifies changes in or additions to systems of record and contains such other information concerning the administration of the Act as may be necessary or useful to Congress for reviewing the effectiveness of the Act in fulfilling its purpose.[431]

4.2.3.4 Oversight by Congress

The task of reviewing the effectiveness of the Act in Congress[432] was taken up in the House of Representatives by a subcommittee of the Committee on Government Operations, namely the Subcommittee on Government Information, Justice, and Agriculture.[433] In the Senate this function was taken up by a subcommittee of the Committee on Governmental Affairs, namely the Subcommittee on Oversight of Government Management.[434] Although Congress in general demonstrates a lack of interest in the Privacy Act, it does from time to time commission various studies of privacy issues from so-called service groups.[435]

---

430 Initially the President had to report annually to Congress. In 1988 s 7(f) of Pub L 100–503 (Computer Matching and Privacy Protection Act) substituted "biennially" for "annually".

431 5 USC s 552a(s)(1)–(4). The report is prepared by the OMB (see par 4.2.3.2).

432 According to Flaherty *Surveillance societies* 319, the OMB perceives itself as sharing parallel oversight responsibility with subcommittees of Congress. The Act itself is silent on the matter. Flaherty is of the opinion that it is difficult to rely on Congressional committees to oversee the Act, since they are "political creatures, burdened with all the usual political concerns of elected representatives", making it "very difficult to persuade them to give sustained attention to any one issue. The saving grace in most cases is that each of these subcommittees has a few talented staff members who perform essential functions".

433 Flaherty *Surveillance societies* 319.

434 Flaherty *Surveillance societies* 319.

435 Such as the Congressional Research Service, the Office of Technology Assessment and the General Accounting Office (Flaherty *Surveillance societies* 319–320).

4.2.3.5 Oversight by courts

Federal agencies are subject to a civil suit for any damage which occurs as a result of wilful or intentional action which violates any individual's rights under the Privacy Act.[436] Officers or employees of agencies may also be found guilty of a misdemeanour and fined for unauthorised disclosure of information or for maintaining a system of records without complying with the requirements laid down by the Act.[437] Bennett argues that the creation of individual rights and the reliance on the courts to ensure the exercise of those rights is the only method of regulation.[438] Most commentators are sceptical about the role of the courts in enforcing the Act. The prevailing view is that the Act is unenforceable in the courts.[439]

4.2.3.6 Conclusion

The system of agency self-enforcement with administrative supervision by the Office of Management and Budget is one of the main weaknesses of the Act. The fact that an independent Federal Privacy Board was not established by the Privacy Act is a serious shortcoming.[440] Initiatives to establish such

436 5 USC s 552a(g). See par 4.2.2.13.

437 5 USC s 552a(i). See par 4.2.2.13.

438 Bennett *Regulating privacy* 173. Dependence on litigation to enforce significant parts of the Act reflects the litigiousness of American society (Flaherty *Surveillance societies* 315). Kirby 1987 *U Cin LR* 745, 757 points out that a system relying on protection through the courageous individual falls short of providing effective relief against all of the implications of the new technology. See also Southard 1989 *Computer/LJ* 359, 372.

439 According to Ronald Plesser, a practitioner in this field, "(t)he Privacy Act, to a large extent, is unenforceable by an individual, because courts have decided that it contains no injunctive relief; the plaintiff has to show that the government acted in a wilful or intentional manner; the plaintiff may have to prove substantial physical injury; and lastly because the act's exemptions are overly broad". (Quoted in Flaherty *Surveillance societies* 343). The end result is that litigation is expensive and complex (Flaherty *Surveillance societies* 315).

440 See Ehlke 1985 *J Mar LR* 829, 846; Simitis 1987 *U Pa LR* 707, 742; Rotenberg 1991 *Gov Inf Q* 79; Gellman 1994 *Gov Inf Q* 245, 247; Schwartz 1995 *Vand LR* 295, 341; Gellman 2000 *Gov Inf Q* 235 who all argue for the establishment of a data protection authority in the United States. Flaherty *Surveillance societies* 365 enumerates the responsibilities and functions a privacy protection commission in the US should have as follows:

(continued...)

an agency have been introduced repeatedly since 1977, but no action has been taken so far.[441]

4.2.4 Relationship between the Freedom of Information Act and the Privacy Act

The Freedom of Information Act (FOIA)[442] was enacted in 1966 to promote open government. It mandates disclosure of government records to any person requesting such disclosure, except if such records are specifically exempted by the FOIA,[443] in which case the agency may choose not to disclose

440(...continued)

1. Articulating privacy concerns in every relevant situation, functioning essentially as an alarm system for the protection of personal privacy.
2. Carrying out oversight to protect the privacy interests of individuals in all federal information-handling activities.
3. Implementing statutory duties under a revised Privacy Act.
4. Conducting investigations and audits of information systems to monitor compliance with the provisions of a revised Privacy Act.
5. Developing and monitoring the implementation of appropriate security guidelines and practices for the protection of personal information in federal hands.
6. Advising and developing regulations appropriate for specific types of personal information systems. Staff members of the proposed privacy protection commission could thus become specialists in different types of information systems and information flows.
7. Monitoring and evaluating developments in information technology with respect to their implications for personal privacy.
8. Conducting research and reporting on all types of privacy issues in the United States.

441 See Gellman 1993 *Softw LJ* 199, 207. An attempt to introduce a Data Protection Board was made in 1989 and 1991 by Congressman Wise, who urged the establishment of a Data Protection Board (HR 3669, 101st Cong, 1st Sess (1989) and HR 685, 102 Cong, 1st Sess (1991)). See also Wise 1991 (March / April) *TDR* 41–44 where his statement delivered in the House of Representatives in connection with the introduction of the Data Protection Act of 1991 (HR 685) is reprinted. The Bill is reproduced in Madsen *Personal data protection* 887–892.

442 Pub L No 89–554, 80 Stat 383 (1966), codified at 5 USC s 552.

443 The Privacy Act provides individuals with a means of access similar to that of the FOIA. The statutes do overlap, but not entirely. The FOIA is entirely an access statute; it permits "any person" to seek access to any "agency record" that is not subject to any of its nine exemptions or its three exclusions. By comparison, the Privacy Act permits only an "individual" to seek access to his or her own "record", and only if that record is maintained by the agency within a "system of records", subject to ten Privacy Act exemptions. Thus, the primary difference between the FOIA and the access provision of the Privacy Act is in the scope of information requestable under each statute. The two Acts should not be considered to be in conflict. According to the PPSC, the two Acts "mesh well. There are no statutory conflicts" (Privacy Commission Report 520). The FOIA also serves to protect the privacy of individuals, in that it gives a right of subject access to records, and it exempts records from access by third parties if this would involve a "clearly unwarranted invasion of privacy" (see Michael *Privacy and human rights* 84). Also see Schwartz (continued...)

the records.[444] There are nine exemptions:[445]

- ❒ records specifically authorised (under criteria established by executive order) to be kept secret in the interests of national defence or foreign policy
- ❒ records related solely to the internal personnel rules and practices of an agency
- ❒ records specifically exempted from disclosure by statute[446]
- ❒ trade secrets and commercial or financial information obtained from a person and considered privileged or confidential[447]
- ❒ inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency
- ❒ personnel, medical and similar files, the disclosure of which would be a clearly unwarranted invasion of personal privacy[448]
- ❒ records or information compiled for law-enforcement purposes[449]

443(...continued)
1995 *Iowa LR* 553 592–595 and ch 8 par 4.2.3.

444 Agencies are not obliged to withhold information if one of these exemptions applies (*Chrysler Corp v Brown* 441 US 281 (1979)).

445 5 USC s 552(b)(1)–(9).

446 Subsequently referred to as exemption three of the FOIA.

447 According to Michael *Privacy and human rights* 84, this provision "comes close to providing a measure of protection for the privacy of legal persons".

448 See fn 443.

449 But only to the extent that the production of such law enforcement records or information: (a) could reasonably be expected to interfere with enforcement proceedings; (b) would deprive a person of a right (continued...)

- records contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions

- geological and geophysical information and data, including maps, concerning wells

After the enactment of the Privacy Act in 1974, the question arose whether an individual could gain access to records kept on him or her under the FOIA, in a case where he or she could not gain access under the Privacy Act,[450] or whether an agency could in such circumstances rely on exemption three of the FOIA[451] to deny access.

Initially the OMB advised that an individual was to be accorded maximum access under both statutes,[452] but when conflicting decisions[453] appeared on the issue the OMB next advised that the Privacy Act was an FOIA exemption three statute,[454] and that an individual who was denied access under a Privacy Act exemption could be denied access under the FOIA as well.[455] This resulted in the anomaly that a third party could gain access to a record on an individual under the FOIA, whereas the individual himself or herself could be denied access to the same record. Before the Supreme Court

449(...continued)
to a fair trial or an impartial adjudication; (c) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (d) could reasonably be expected to disclose the identity of a confidential source; (e) would disclose techniques and procedures for law enforcement investigations or prosecutions, (f) could reasonably be expected to endanger the life or physical safety of any individual (5 USC s 552(b)(7)).

450 Eg, because one of the exemptions of the Privacy Act was applicable.

451 See fn 446.

452 See 40 Fed Reg 56742 (1974).

453 In *Shapiro v Drug Enforcement Admin* 721 F 2d 215 (7th Cir 1983) it was held that an individual was confined to the Privacy Act in seeking access to his own records; *contra Porter v Dept of Justice* 717 F 2d 787 (3rd Cir 1983).

454 See fn 446.

455 See 49 Fed Reg 12248, 12338 (1984).

could resolve the issue,[456] Congress enacted the Central Intelligence Agency Information Act ("CIA Act") in October 1984.[457] This Act amended the Privacy Act by adding a subsection,[458] the effect of which is that an individual may proceed under both the Privacy Act and the FOIA to gain access to his or her records, and he or she must be afforded maximum access under both statutes.[459]

4.2.5 Privacy Protection Study Commission

Section 5 of Public Law 93–579[460] provides for the establishment of a Privacy Protection Study Commission (PPSC)[461] consisting of seven members, chosen for their expertise in "civil rights and liberties, law, social sciences, computer technology, business, records management, and state and local government".[462]

The Commission had a broad mandate to study data banks, automated data processing programs, and the information systems of governmental, regional, and private organisations[463] to determine what standards and procedures for the protection of personal information were being enforced. It then had to recommend to the President and Congress the extent, if any, to which the requirements of the Privacy Act should be applied to the information practices of those organisations by legislation, administrative action or voluntary adoption of such requirements and principles. The commission could also

456 *Dept of Justice v Provenzano* 104 S Ct 1706 (1984). This would have been one of the first cases under the Privacy Act that the Supreme Court would have heard.

457 Pub L No 98–477, 98 Stat 2209 (1984), codified at 50 USC s 401.

458 5 USC s 225a(q)(2). After insertion of the CMPPA, the section was renumbered s 225a(t)(2).

459 See eg *Savada v US Dept of Defense* 755 F Supp 6 (DDC 1991); *Blazy v Tenet* 979 F Supp 10 (DDC 1997) (quoting subsection (t)(2) and stating that "[d]ocument requests therefore must be analyzed under both Acts"). Also see Schwartz 1995 *Iowa LR* 553, 592–595.

460 This section was not codified with the rest of the Privacy Act.

461 The PPSC was part of the compromise reached in order to pass a law during the 1974 session. See Bennett *Regulating privacy* 172 and par 4.2.1.5.

462 Pub L No 93–579 s 5(a)(1).

463 Except information systems maintained by religious organisations (Pub L 93–579 s 5(c)(2)(C)).

recommend other legislation it deemed necessary to protect the individual's privacy, while meeting the legitimate needs of government and society for information.[464]

The Commission was further specifically instructed to study mailing lists, the use of a universal identifier, the use of IRS data, and the adequacy of the provisions of the Privacy Act itself.[465] It was authorised to consider personal information activities relating to medical, insurance, education, employment, credit, and banking records.[466] It was also authorised to hold hearings, conduct inspections, and issue subpoenas to carry out its functions.[467]

The Commission delivered its report to President Carter and Congress in 1977,[468] and then ceased to exist.[469] It thought that individuals have a compelling interest in records that organisations keep on them, but that that interest is poorly protected. The Commission concluded that an effective privacy protection policy should have the following three objectives:

- ❒ minimising intrusiveness[470]

464 Pub L No 93–579 s 5(b)(2).

465 Pub L No 93–579 s 5(c).

466 Pub L No 93–579 s 5(c)(2)(A).

467 Pub L No 93–579 s 5(e)(1).

468 PPSC *Personal privacy in an information society: the report of the Privacy Protection Study Commission* (1977) (cited as Privacy Commission Report).

469 See also Gellman 1993 *Softw LJ* 199, 216–220.

470 This entails reaching a proper balance between what an individual is expected to divulge to a record-keeping organisation and what he or she seeks in return. Four ways to address this issue are recommended:
(a) Individuals should be informed more fully about the information needs and practices of record-keeping organisations in advance of committing themselves to a relationship with them.
(b) Certain information should not be collected at all, eg in the employment and personnel area, arrest information should not be collected for hiring and promotion decisions, unless its use for such purposes is required by law.
(c) There should be limitations on the methods used to collect information, and private sector record keepers should be required to exercise reasonable care in selecting and retaining other organisations to collect information on their behalf.
(d) In some areas, as a last resort, there should be a governmental mechanism to receive complaints about

(continued...)

- ❒ maximising fairness[471]
- ❒ creating a legitimate enforceable expectation of confidentiality[472]

The Commission followed three implementation choices:[473]

- ❒ voluntary compliance with its recommendation in areas where the need for the recommended change is not acute, or if the industry has shown itself willing to cooperate voluntarily[474]
- ❒ mandatory implementation in the private sector, such as the credit, insurance and depository industry, by creating "legitimate expectations of confidentiality" enforceable by either individual

470(...continued)
the propriety of inquiries made of individuals, as well as to bring them to the attention of bodies responsible for establishing public policy (Privacy Commission Report 16–17).

471 This entails that record-keeping organisations should be opened up in ways that will minimise the extent to which recorded information about an individual is itself a source of unfairness in any decision about him or her made on the basis of it. Recommendations in this regard include:
(a) Applicants should be appraised of the scope, sources, and methods of inquiry the organisation intends to use in verifying application information.
(b) Individuals should be given a general right of access to records on them maintained by insurance institutions and medical-care providers, and a more limited right of access (triggered by an adverse decision) in the case of records maintained by credit and depository institutions.
(c) There should be a right to correct and amend a record, coupled with the obligation on record-keeping organisations to forward the correction to the past recipients of incorrect information.
(d) In regard to fairness in disclosure, it is sometimes a necessary protection that the individual should have to authorise such disclosure, and this should be coupled with the principle of limited disclosure and the requirement that reasonable procedures to assure accuracy, timeliness and completeness of records be introduced (Privacy Commission Report 18–19).

472 This entails creating and defining obligations with respect to the use that will be made of information on an individual and how such information will be disclosed. To help redress the imbalances between individuals and organisations on the one hand, and organisations, individuals and government on the other, it is recommended that a legally enforceable "expectation of confidentiality" be created in several areas (Privacy Commission Report 19–20).

473 The PPSC contended that the strongest argument for using a combination of alternatives is the dynamic character of personal-data record-keeping practices which will continue to create new privacy concerns, and redirect existing ones (Privacy Commission Report 35).

474 Privacy Commission Report 34–35.

or governmental action[475]

- the creation of a federal body to oversee, regulate, and enforce compliance with certain of the Commission's recommendations[476]

An independent entity within the federal government could also fulfil the need for a mechanism to interpret both law and policy.[477] The entity should be charged with the responsibility for performing the following functions:[478]

- to monitor and evaluate privacy statutes and regulations enacted pursuant to the recommendations of the PPSC, and have the authority to formally participate in any federal administrative proceedings or process where the action being considered by another agency would materially affect the protection of personal privacy, either because of direct government action or because of government regulation of others

- to continue privacy research, study and investigations and to supplement other governmental mechanisms through which citizens could question the propriety of information collected and used by various segments of the public and private sector

- to issue rules interpreting the Privacy Act

- to act as an advisory board on privacy to the federal government and the states

475 Privacy Commission Report 34–35.

476 Privacy Commission Report 35.

477 Privacy Commission Report 36.

478 Privacy Commission Report 37.

To date no federal legislation based on the recommendations of the PPSC has been enacted.[479]

4.2.6 Summary

The purpose of the Privacy Act is to balance the government's need to maintain information about individuals against the right of individuals to be protected from unwarranted invasion of their privacy stemming from federal agencies' collection, maintenance, use and disclosure of personal information about them. As was previously demonstrated, the historical context of the Act is important in understanding of its remedial purposes. Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal; it was also concerned with potential abuses arising from the government's increasing use of computers to store and retrieve personal data by means of a universal identifier such as an individual's social security number.

The Act focuses on four basic policy objectives:[480]

- ❒ to restrict disclosure of personally identifiable records maintained by agencies
- ❒ to grant individuals increased rights of access to agency records maintained on themselves
- ❒ to grant individuals the right to seek amendment of agency records maintained on themselves after demonstrating that the records are not accurate, relevant, timely or complete

479 A number of legislative bills were introduced in Congress, primarily by Representatives Goldwater and Koch, both of whom had been members of the PPSC (Bigelow 1986 *InfAge* 134). Also see fn 441. Flaherty *Surveillance societies* 309 ascribes the poor results that the PPSC's report had on the private and public sector to the Carter administration's failure to settle its own privacy agenda and then to sell it to Congress. The so-called "Carter Privacy Initiative" proposed four bills providing protection for medical records, federally funded research records, financial records, and news media notes and materials. Although major hearings took place, almost no legislation was enacted before the electoral defeat of Carter, except for the Right to Financial Privacy Act of 1978 (see fn 127). (The Privacy Protection Act of 1980 (see fn 134), designed to control government searches of newsrooms, was not a product of the PPSC – Flaherty *Surveillance Societies* 451 fn 11.) The Reagan administration perceived no need to take privacy initiatives; in fact it was committed to reduce government, not expand it. Consequently, efforts to introduce privacy legislation in Congress have been thwarted by the Reagan administration (Shattuck 1984 *Hastings LJ* 991, 997).

480 See also US Dept of Justice *Overview of the Privacy Act*.

- to establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance and dissemination of records

However, enforcement of the Act is hampered by a weak remedial scheme and the lack of a proper data protection authority.

4.3 Fair Credit Reporting Act of 1970

4.3.1 Background and legislative history

The FCRA was the first attempt by Congress to control the use of personal information within the private sector, and is also considered to be Congress's most significant effort to regulate data collection and transference between private parties.[481] Growing Congressional concern about the threat posed to personal privacy led to Congressional hearings during the 1960s by the Government Operations Committee of the House of Representatives.[482] Late in 1964 a Special Subcommittee on Invasion of Privacy was created by the chairman of the Government Operations Committee. This subcommittee held hearings in 1968 on the privacy abuses inherent in the operation of private commercial credit reporting organisations.[483] Choosing to deal with privacy problems on a piecemeal or "as needed" basis, Congress enacted the Fair Credit Reporting Act (FCRA) in 1970.[484] It was directed to dealing

481 See Graham 1987 *Tex LR* 1395, 1421 fn 142; Hixson *Public society* 219.

482 See par 4.2.1.2.

483 US House of Representatives Hearing Before the Special Subcommittee on Invasion of Privacy: *Commercial Credit Bureaus* 90th Cong 2d Sess (1968).

484 Pub L No 91–508, 84 Stat 1136 (1970), codified at 15 USC s 1681. The FCRA is a subdivision of the Consumer Credit Protection Act (CCPA), 15 USC s 1601 *et seq*. Other statutes that form part of the CCPA are the Equal Credit Opportunity Act (ECOA), 15 USC s 1691, the Truth in Lending Act (TILA), 15 USC s 1601, and the Electronic Fund Transfer Act (EFTA) 15 USC s 1693. Although only the FCRA was primarily intended to be a privacy act, the other subdivisions of the CCPA also have privacy implications, both positive and negative. The CCPA is a statute designed to regulate the flow of information in consumer credit transactions, and seen from such a perspective the information privacy implications becomes obvious: More information on the consumer is actually generated.

The ECOA is intended to prevent discrimination in lending practices by prohibiting a creditor from asking a credit applicant to disclose sex, race, colour, religion, national origin, birth-control practices, or

(continued...)

with many privacy abuses uncovered by the Subcommittee hearings. However, the final version of the FCRA was quite different from the original bill introduced almost a year earlier, representing a compromise with the credit industry.[485] As a consequence the FCRA had many loopholes and had to be amended in 1996 by the Consumer Credit Reporting Reform Act.[486]

4.3.2 Provisions of FCRA

4.3.2.1 Purpose of FCRA

Although the FCRA's main concern is to ensure fair and accurate credit reporting on an individual, it is also concerned with the privacy implications for the individual subjected to a credit investigation and consumer report. While acknowledging on the one hand the vital role of consumer reporting agencies

484(...continued)
child-rearing plans. The spin-off of this for privacy is that sensitive personal information is kept out of a creditor's records.

The EFTA's primary objective is to protect individual consumer rights by providing a framework that establishes the rights, liabilities and responsibilities of consumers, financial institutions and intermediaries. On the positive side for privacy, EFTA requires the financial institution to inform electronic fund transfer system users under what circumstances the financial institution will in the ordinary course of business disclose information concerning the user's account to third persons. On the negative side for privacy, however, is the fact that EFTA requires financial institutions to provide the consumer with written documentation of all transfers of funds initiated from an electronic terminal. The amount involved, date of transfer, type of transfer, the identity of the consumer's account with the financial institution from or to which funds are transferred, the identity of any third party to or from whom funds are transferred and the location or identification of the electronic terminal involved must all be documented. This required documentation forces banks and other financial institutions to create records and information flows on individuals where none existed before.

The purpose of the TILA is to give consumers transactional information to prevent the uninformed use of credit. This includes both initial disclosures by the creditor when an open-end account is involved and periodic statements giving information about specific credit transactions. As in the case of EFTA, these requirements of the TILA have negative implications for the consumer's information privacy, in that more information on the consumer is generated.

Part of the TILA is the Fair Credit Billing Act (FCBA – 15 USC s 1666). The FCBA provides a mechanism by which disputed entries on monthly statements can be challenged. This provides the consumer with the opportunity to correct errors, as they appear on the statement, in his or her credit files, and therefore benefits information privacy.

On the CCPA, see Roos 1990 *TSAR* 477, 481–482; Rasor 1986 *J Mar LR* 941. See also Rubin *Private rights* 107.

485 See Blair & Maurer 1984 *Mo LR* 289, 302.

486 See Cate *Information age* 82.

for the banking system,[487] Congress also emphasised the need to ensure that these agencies exercise their responsibilities with fairness, impartiality and a respect for the consumer's right to privacy.[488]

It is consequently the stated purpose of the FCRA that "consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information..."[489]

The FCRA reflects three broad goals:[490]

- the reduction of secrecy in credit reporting
- the reduction of potential harm to the consumer by allowing the consumer to amend errors in the files
- the increase of accuracy in credit reports

4.3.2.2 Scope of FCRA: definitional framework

The scope of the FCRA is determined by the definitions assigned to key terms used in the Act. The FCRA protects **consumers** against unfair credit reporting (by means of **consumer reports** or **investigative consumer reports**) by **consumer reporting agencies** to third parties, because of disputed information in the **files** kept by the agency on the consumer.

a Consumer

The FCRA is concerned with the rights of consumers. The term "consumer" refers by definition to an

487 15 USC s 1681(a)(1) & (3).

488 15 USC s 1681(a)(4).

489 15 USC s 1681(b).

490 Blair & Maurer 1984 *Mo LR* 289, 303–305.

individual.[491] This would lead one to conclude that the FCRA only gives rights to natural persons and not to juristic persons.[492]

b Consumer report

The definition of a consumer report is important in determining the scope of the Act, because reports that fall outside this definition are not regulated by the FCRA. A consumer report is defined as any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.[493] Up to this point the definition is so broad that it would include almost any information that relates to the consumer. However, the definition limits itself by requiring that this information must be used or expected to be used or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance (to be used primarily for personal, family, or household purposes), or for employment purposes,[494] or for other purposes authorised under the FCRA.[495]

The following reports are not consumer reports falling under the FCRA:

- a report containing information solely as to transactions or experiences between the consumer

491 15 USC s 1681a(c). See also fn 506.

492 A business does not qualify as a "consumer" and a consumer's business transactions or so-called "commercial credit report" are not covered by the FCRA (*Ley v Boron Oil Co* 419 F Supp 1240 (DC Pa 1976); *Sizemore v Bambi Leasing Corp* 360 F Supp 252 (DC Ga 1973)). For criticism of this aspect, see Petroceli *Low profile* 56.

493 Reidenberg 1992 *Fed Com LJ* 195, 211 criticises the "expansive categories of regulated personal information", because the implication is that "excessive personal information may be collected" by credit reporting agencies.

494 Employment purposes also mean evaluating a consumer for employment, promotion, reassignment or retention as an employee (15 USC s 1681a(h)).

495 15 USC s 1681a(d)(1). See *Emerson v JF Shea Co* 76 Cal App 3d 579 (1978).

and the person making the report[496] (in other words, creditors that do not provide third parties with information may keep records on their customers and conduct investigations without falling under the FCRA[497])

- an authorisation or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device[498]

- a report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his or her decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the disclosures to the consumer required under section 1681m[499]of the FCRA[500]

- excluded communications as described in subsection (o) (that is, reports by employment agencies)[501]

---

496 Or communication of that information among persons related by common ownership or affiliated by corporate control. In such a situation the consumer must be informed that the information may be communicated among such persons and be given the opportunity before the time to prevent this (15 USC s 1681a(d)(2)(A)(iii). 15 USC s 1681a(d)(2)(A)(i)–(iii)).

497 Eg, a bank that reports that a customer is delinquent in a credit card account is not acting as a consumer reporting agency (*Smoth v First Nat Bank* 837 F 2d 1575 (CA Ga 1998)). Also see *Rush v Macy's New York, Inc* 775 F 2d 1554 (CA Fla 1985) and fn 508 below.

498 15 USC s 1681a(d)(2)(B).

499 On s 1681m, see text to fn 598.

500 15 USC s 1681a(d)(2)(C).

501 15 USC s 1681a(d)(2)(D). Excluded communications are defined in 15 USC s 1681a(o) as an investigative consumer report that is made to a prospective employer for the purpose of procuring an employee for the employer or procuring an opportunity for a natural person to work for the employer. Such report should be made by a person who regularly performs such procurement, and not be used by any other person for any other purpose. Further requirements are that the consumer has consented to such report, the inquiries made for purposes of the report do not violate any applicable equal employment opportunity law or regulation, and the person who makes the communication discloses at the request of the consumer the nature and substance of all information in the consumer's file at the time of the request, except the sources of any information that is acquired solely for use in making the communication and is actually used for no

(continued...)

c Investigative consumer report

The term "investigative consumer report" is defined as a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbours, friends, or associates of the consumer reported on, or with others with whom he or she is acquainted or who may have knowledge concerning any such items of information. However, such information does not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency, when such information was obtained directly from a creditor of the consumer or from the consumer.[502]

In other words, an investigative consumer report is also a consumer report and must meet the definition of a consumer report, but the information in this type of consumer report is obtained through personal interviews with neighbours or friends, and not from a creditor of the consumer or from the consumer himself or herself. One would expect that information obtained in this manner should be treated with more caution, and the FCRA therefore contains special provisions for this type of report.[503]

d Consumer reporting agency

The FCRA defines the term "consumer reporting agency" as any person[504] who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and who uses any means or facility of interstate

501(...continued)
other purpose. The person must also notify the consumer who is the subject of the communication, in writing, of the consumer's right to request such information.

502 15 USC s 1681a(e).

503 See further par 4.3.2.5 and also see Sherland 1984 *Wash LR* 401 *et seq*.

504 A federal agency, such as the FBI, is not a consumer reporting agency (*Ollestad v Kelley* 573 F 2d 1109 (CA Cal 1978)).

commerce[505] for the purpose of preparing or furnishing consumer reports.

A "person" is defined as being any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.[506] In other words, a consumer reporting agency can be either a natural person or a juristic person.

e File

The term "file", when used in connection with information on a consumer, means all the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.[507] In other words, the FCRA is equally applicable to information stored in a paper or computer file.

f Summary

To sum up, the Fair Credit Reporting Act gives rights to individuals only, it imposes obligations on consumer reporting agencies in the private sector, and it applies to personal information in either a paper file or a computer file that is to be used for credit, insurance or employment purposes.

4.3.2.3 Permissible purposes in disclosing consumer reports

a In general

The FCRA regulates the disclosure of credit reports by consumer reporting agencies to third parties,

505 15 USC s 1681a(f). The requirement that a consumer reporting agency must be involved in interstate commerce is necessary in order for the agency to be subject to the FCRA, since it is a federal piece of legislation. On the commerce clause, see also fn 116.

506 15 USC s 1681a(b). A person is thus interpreted as including juristic persons, but it is important to note that "persons" are not protected under the FCRA; only "consumers" are protected. A consumer must be a natural person.

507 15 USC s 1681a(g).

by providing that such information may only be disclosed in certain circumstances. In other words, the FCRA does not regulate all creditors, but only regulates third party providers. Creditors that do not provide third parties with information may keep records on their customers and conduct investigations without falling under the FCRA.[508]

The circumstances under which a consumer report may be furnished to a third party are:[509]

- pursuant to a court order or a subpoena issued by a federal grand jury[510]
- in accordance with the written instructions of the consumer to whom it relates (in other words, where the consumer has consented to such disclosure)[511]
- to a person whom the reporting agency has reason to believe intends to use the report for the following purposes:
  - in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer[512]

508 Rubin *Private rights* 126 considers this to be a serious flaw in the FCRA. The FCRA also does not in general regulate the collection of personal information, or the acquisition of excessive personal information (see Reidenberg 1992 *Fed Comm LJ* 195, 211).

509 15 USC s 1681b(a).This subsection is subject to 15 USC s 1681b(c) dealing with the furnishing of a report in connection with credit or insurance transactions that are not initiated by the consumer (see par 4.3.2.3.c).

510 15 USC s 1681b(a)(1).

511 15 USC s 1681b(a)(2).

512 15 USC s 1681b(a)(3)(A). 15 USC s 1681b(c) contains further conditions for furnishing consumer reports in connection with credit transactions that were not initiated by the consumer. This subsection will be discussed in par 4.3.2.3.c.

– for employment purposes[513]

– for the underwriting of insurance involving the consumer[514]

– in the determination of the eligibility of the consumer for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status[515]

– as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation[516]

– in response to a legitimate business need for the information in connection with a business transaction that has been initiated by the consumer, or to review an account to determine whether the consumer is continuing to meet the terms of the account[517]

513 15 USC s 1681b(a)(3)(B). "Employment purposes" in this regard means not only the granting of employment, but also evaluation for promotion, reassignment or retention as an employee (15 USC s 1681a(h)). If the consumer report contains public record information (eg information relating to arrests, indictments, convictions, suits, tax liens and outstanding judgments) and is likely to have an adverse effect upon a consumer's ability to obtain employment, the agency must either inform the consumer about it, or maintain strict procedures to ensure that the information is complete and up to date (15 USC s 1681k(a)). National security investigations are exempted from this provision (15 USC s 1681k(b)). 15 USC s 1681b(b) contains further conditions for furnishing and using consumer reports for employment purposes and will be discussed in par 4.3.2.3.b. Also see Cooper 1998 *Employee Relations LJ* 57.

514 15 USC s 1681b(a)(3)(C). 15 USC s 1681b(c) contains further conditions for furnishing consumer reports in connection with insurance transactions that are not initiated by the consumer. This subsection will be discussed in par 4.3.2.3.c.

515 15 USC s 1681b(a)(3)(D).

516 15 USC s 1681b(a)(3)(E).

517 15 USC s 1681b(a)(3)(F). Initially the FCRA only required "a legitimate business need". This was severely criticised by commentators (see Hixon *Public society* 220; Soma & Wehmhoefer 1983 *Denver LJ* 449, 464; Petrocelli *Low profile* 42; Rubin *Private rights* 126; Privacy Commission Report 86). The PPSC recommended that the FCRA be amended to provide that information on an individual maintained by a credit bureau may only be used for credit-related purposes (Privacy Commission Report 87). The section was subsequently amended to include the reference to business transactions and review of accounts

(continued...)

- in response to a request by the head of a state or local child support enforcement agency if it is certified that the consumer report is required for the purpose of establishing an individual's capacity to make child support payments or determining the appropriate level of such payments[518]

- to an agency administering a state plan for child and spousal support[519] for use to set an initial or modified child support award

A consumer reporting agency may also furnish identifying information respecting any consumer, limited to the name, address, former addresses, places of employment, or former places of employment, to a governmental agency, despite the prohibition on disclosure of consumer reports.[520]

These circumstances listed may be considered lawful purposes for the disclosure of personal credit information.[521]

b Conditions for furnishing and using consumer reports for employment purposes

The FCRA does not prohibit the furnishing and use of a consumer report for employment purposes, but the Act does impose additional requirements. Before a person may procure a consumer report for employment purposes, such person must make a clear and conspicuous disclosure in writing to the

517(...continued)
relating to the consumer.

518 15 USC s 1681b(a)(4). It should also be certified that the paternity of the consumer to whom the obligation relates has been established or acknowledged, that the consumer has received notice that the report will be requested, and the consumer report will be kept confidential and will not be used for any other purposes than those described.

519 Under 42 USC s 654. See Schwartz 1992 *Hastings LJ* 1321, 1367 *et seq*.

520 15 USC s 1681f.

521 See ch 7 par 2.3.2.3.

consumer, in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes, and the consumer must authorise in writing (for example on the document) the procurement of the report by that person.[522]

A consumer reporting agency may furnish a consumer report for employment purposes only if the user of the report has certified that such user has fulfilled its obligation under this section to inform the consumer about the procurement of the report and also certifies that the information contained in the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation. The consumer reporting agency must also provide, together with the report, a summary of the consumer's rights under the FCRA.[523]

Before taking any adverse action[524] based in whole or in part on a consumer report for employment purposes, the person intending to take such adverse action must furnish the consumer to whom the report relates with a copy of the report and a written description of the consumer's rights under the FCRA.[525] National security investigations are exempted from this requirement.[526]

---

522 15 USC s 1681b(b)(2)(A). Special provisions exist for applications by mail, telephone or computer (see 15 USC s 1681b(b)(2)(B)). For a discussion of the obligations imposed on employers by the FCRA, see Cooper 1998 *Employee relations LJ* 57; Paddock 1998 *Colorado L'yer* 95.

523 15 USC s 1681b(b)(1).

524 Adverse action in this regard means a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee (see 15 USC s 1681a(k)(1)(B)(ii)).

525 15 USC s 1681b(b)(3)(A). Special provisions exist for applications by mail, telephone or computer (see 15 USC s 1681b(b)(3)(B)).

526 See 15 USC s 1681b(b)(4). The term "national security investigation" means any official inquiry by an agency or department of the US government to determine the eligibility of a consumer to receive access or continued access to classified information or to determine whether classified information has been lost or compromised (see 15 USC s 1681b(b)(4)(E)(i)). Detailed rules surround this exception, *inter alia* that the head of an agency relying on this exception must make a written finding that there is reason to believe that compliance with subpar (3) will (a) endanger the life or physical safety of any person; (b) result in flight fromprosecution; (c) result in the destruction of, or tampering with, evidence relevant to the investigation; (d) result in the intimidation of a potential witness relevant to the investigation; (e) result in the compromise of classified information; or (f) otherwise seriously jeopardise or unduly delay the investigation or another official proceeding.

A consumer reporting agency may not furnish for employment purposes, or in connection with a credit or insurance transaction, a consumer report that contains medical information about a consumer, unless the consumer consents to the furnishing of the report.[527]

c Furnishing reports in connection with unsolicited credit or insurance transactions

A consumer reporting agency may not furnish a consumer report relating to a consumer in connection with an unsolicited credit or insurance transaction[528] unless the consumer authorises the agency to provide such report.[529]

Where the consumer has not authorised the consumer report, creditors and insurers may still use "file information" (the name and address of the consumer, an identifier that is not unique to the consumer and that is used by the person solely for the purpose of verifying the identity of the consumer, as well as other information pertaining to a consumer that does not identify the relationship or experience of the consumer with respect to a particular creditor or other entity),[530] to send out unsolicited credit and insurance offers. However, the FCRA imposes conditions in such a case:[531]

- ❒ the transaction must consists of a firm offer of credit or insurance[532]

- ❒ the consumer reporting agency must have complied with subsection (e) of this section

527 15 USC s 1681b(g).

528 This does not include the use of a consumer report by a person with whom the consumer has an account or insurance policy, for purposes of reviewing the account or insurance policy, or collecting the account (15 USC s 1681a(m)).

529 15 USC s 1681b(c)(1)(A).

530 15 USC s 1681b(c)(2).

531 15 USC s 1681b(c)(1)(B).

532 The Act contains a lengthy definition of "a firm offer of credit or insurance" (see 15 USC s 1681a(l)).

- the consumer must not have elected, in accordance with subsection (e) of this section, to have his or her name and address excluded from lists of names provided by the agency pursuant to this paragraph[533]

In terms of subsection (e) of this section, consumers have the right to elect to be excluded from a consumer reporting agency list in connection with unsolicited credit and insurance offers, by notifying the agency that they do not consent to such inclusion.[534] For this purpose, a consumer reporting agency must establish and maintain a notification system, including a toll-free telephone number, which permits any consumer whose consumer report is maintained by the agency to notify the agency, with appropriate identification, of the consumer's election to have his or her name and address excluded from any list.[535] The consumer agency must also annually publish in a publication of general circulation in the area served by the agency a notification that information in consumer files maintained by the agency may be used in connection with such transactions, as well as the address and toll-free telephone number for consumers to use to notify the agency of their election.[536]

d Certain use or obtaining of information prohibited

On the one hand the FCRA regulates the disclosure of credit reports by consumer reporting agencies to third parties, by providing that such information may only be disclosed in certain circumstances. On the other hand, the Act also imposes obligations on the third parties. Third parties may not use or obtain a consumer report for any purpose, unless two requirements are met,[537] namely that the consumer report is obtained for a purpose authorised by the FCRA, and that the prospective user certifies what

533 Persons who make written solicitations for credit or insurance to consumers must also comply with 15 USC s 1681m. See par 4.3.2.9.c.

534 15 USC s 1681b(e)(1).

535 15 USC s 1681b(e)(5)(A)(i).

536 15 USC s 1681b(e)(5)(A)(ii).

537 15 USC 1681b(f).

the purpose of the report is in accordance with the requirements of the FCRA.[538]

4.3.2.4 Requirements relating to information contained in consumer reports

The FCRA not only regulates the disclosure and use of credit reports, it also lays down certain requirements in relation to the content of the reports.

First of all, the reporting of obsolete information is prohibited,[539] unless the consumer report is to be used in connection with a credit transaction involving $150 000 or more, the underwriting of life insurance involving an amount of $150 000 or more, or the employment of an individual at an annual salary or $ 75 000 or more.[540] Obsolete information is any adverse information, other than records of convictions of crimes, which is older than seven years, as well as bankruptcy adjudications more than ten years prior to the consumer report, suits and judgments older than seven years, paid tax liens older than seven years as well as civil suits, civil judgments and records of arrests and convictions that from date of entry antedate the report by more than seven years or until the governing statute of limitations has expired.[541]

Furthermore, if a credit account of a consumer was voluntarily closed by the consumer, the agency must indicate that fact in any consumer report that includes information related to the account.[542] If the information which was furnished to the agency is disputed by the consumer, the agency must also indicate that fact in each consumer report that includes the disputed information.[543] The consumer reporting agency is not required to remove disputed data from the file, unless it is outdated or cannot

538 Ie as required by 15 USC s 1681e (see par 4.3.2.6.a).

539 15 USC s 1681c(a). It is not required that obsolete information should be deleted from the file, however.

540 15 USC s 1681c(b). These amounts were considerably increased in 1996 by the amendments to the FCRA (see par 4.3.1).

541 15 USC s 1681c(a).

542 15 USC s 1681c(e).

543 15 USC s 1681c(f).

be verified.[544]

Notwithstanding any other provision of the FCRA, a consumer reporting agency is obliged to include in a consumer report any information on the failure of the consumer to pay overdue child support. This duty arises where the information is provided to the consumer reporting agency by a state or local child support enforcement agency, or is verified by any local, state or federal government agency and is not older than seven years.[545]

4.3.2.5 Provisions regarding investigative consumer reports

As previously stated, the information in an investigative consumer report is obtained through personal interviews with neighbours or friends, and not from a creditor of the consumer or from the consumer himself or herself and because of that, the information obtained in this manner is treated with more caution. The FCRA therefore imposes additional requirements when this type of report is involved.

First of all, an investigative consumer report may not be procured or caused to be prepared unless it is disclosed in writing to the consumer that such a report, which may include information as to his or her character, general reputation, personal characteristics, and mode of living, may be made.[546] The consumer must also be informed about his or her right to request information about the nature and scope of the investigation,[547] and the disclosure must contain a written summary of the rights of the consumer prepared pursuant to section 1681g(c).[548]

---

544 See discussion in par 4.3.2.8 below.

545 15 USC s 1681s–1.

546 15 USC s 1681d(a)(1). This provision does not place a duty on the agency to disclose the existence of the report, but on the user of the report, ie the creditor. See *Austin v Bankamerica Service Corp* 419 F Supp 730 (5th Cir 1974).

547 15 USC s 1681d(b).

548 15 USC s 1681d(1)(B). On 15 USC s 1681g see par 4.3.2.7.b

The person procuring the report must certify to the consumer reporting agency that such person has made the disclosures to the consumer as required and that the person will comply with the duty to disclose information about the nature and scope of the investigation to the consumer.[549] Should the consumer request in writing information about the investigation, the person procuring the report must make a complete and accurate disclosure of the nature and scope thereof.[550]

A consumer reporting agency may not prepare or furnish an investigative consumer report on a consumer that contains information that is adverse to the interests of the consumer and that was obtained through a personal interview with a neighbour, friend, associate or acquaintance of the consumer, unless the agency has followed reasonable procedures to obtain confirmation of the information from an additional source that has independent and direct knowledge of the information, or where the person interviewed is the best possible source of the information.[551]

Adverse information in an investigative consumer report may not be taken up in a subsequent report, unless the information is part of a public record, or has been verified or is not older than three months.[552]

4.3.2.6 Compliance procedures

The FCRA requires consumer reporting agencies to "maintain reasonable procedures" to ensure that consumer reports are furnished only for permissible purposes (for example for credit, employment or insurance purposes) and do not contain obsolete information. These procedures must require that prospective users of the information identify themselves, certify the purposes for which the information

549 15 USC s 1681d(a)(2) & 15 USC s 1681d(d)(1).

550 15 USC s 1681d(b).

551 15 USC s 1681d(d)(4).

552 15 USC s 1681l.

is sought, and certify that the information will be used for no other purpose.[553] Every consumer reporting agency must make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such consumer report. No consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a permissible purpose.[554]

A consumer reporting agency must also "follow reasonable procedures"[555] when preparing a report to assure "maximum possible accuracy"[556] of the information.[557]

A consumer reporting agency may not prohibit a user of a consumer report furnished by the agency on a consumer from disclosing the contents of the report to the consumer, if adverse action against the consumer has been taken by the user based in whole or in part on the report.[558]

A consumer reporting agency must furnish to any person who regularly and in the ordinary course of business furnishes information to the agency with respect to any consumer, or to whom a consumer

553 See also par 4.3.2.3.d.

554 15 USC s 1681e(a).

555 According to Sherland 1984 *Wash LR* 401, 405, the courts use a two-step analysis to determine whether a consumer reporting agency has violated the "reasonable procedure" requirement. In step one they determine whether the report is substantively accurate. If it is, the agency has a complete defence. If it is not, the court proceeds to step two, which entails determining whether the procedures the agency adopted were reasonable. According to *Bryant v TRW Inc* 689 F 2d 72 (6th Cir 1982) the standard of conduct that is required is that which a reasonably prudent person would observe under the same circumstances, and that goes beyond merely ensuring that the information reported to the agency was accurately relayed. Sherland 405 criticises this approach, contending that Congress intended a consumer reporting agency (as opposed to a consumer investigating agency) to be a mere conduit of information until a consumer disputes information in a credit report and requests an investigation.

556 The FCRA balances the need for fast and accurate information against the difficulties inherent in running a credit agency by requiring "maximum possible accuracy" instead of 100% accuracy (Sherland 1984 *Wash LR* 401, 404).

557 15 USC s 1681e(b). In *Bryant v TRW Inc* 689 F 2d 72 (6th Cir 1982) it was held that under the FCRA liability does not flow automatically from the fact that a credit reporting agency reports inaccurate information. Instead liability flows from failure to follow reasonable procedures to assure maximum possible accuracy of information. Ie, the FCRA does not impose strict liability.

558 15 USC s 1681e(c).

report is provided by the agency, a notice of such person's responsibilities under the FCRA.[559] The Federal Trade Commission prescribes the content of such notices.[560]

A person may not procure a consumer report for purposes of reselling the report[561] unless the person discloses to the consumer reporting agency the identity of the end-user of the report, as well as each permissible purpose for which the report is furnished to the end-user.[562] A person who procures a consumer report for purposes of reselling the report must furthermore establish and comply with reasonable procedures designed to ensure that the report is resold by the person only for a permissible purpose. These procedures must include requiring that each person to whom the report is resold and who resells or supplies the report to another person should identify each end user of the resold report, certify each purpose for which the report will be used, and certify that the report will be used for no other purpose.[563] Before reselling the report, a person must also make reasonable efforts to verify the identifications and certifications.[564]

However, the name of the end user may not be revealed where the end user is a federal government agency or department which procures the report for purposes of determining the eligibility of the consumer to receive access (or continued access) to classified information. The agency or department must certify in writing that nondisclosure is necessary to protect classified information or the safety of certain persons.[565]

559 15 USC s 1681e(d)(1).

560 15 USC s 1681e(d)(2).

561 A reference to "a report" should be understood to include any information in the report.

562 15 USC s 1681e(e)(1).

563 15 USC s 1681e(e)(2)(A).

564 15 USC s 1681e(e)(2)(B).

565 15 USC s 1681e(d)(3).

4.3.2.7 Disclosures to consumers by consumer reporting agency

a Information on file; sources; recipients

The FCRA does not require of consumer reporting agencies to inform consumers that they have files on them. However, it does require that a consumer reporting agency must, if requested, disclose to a consumer, who has properly identified himself or herself,[566] all information in the consumer's file at the time of the request.[567] Such disclosure must be made in writing, or in another form authorised by the consumer and available from the agency.[568] Trained personnel must be provided to explain to the consumer any information furnished to him or her.[569] The consumer may also be accompanied by one other person of his or her choice.[570]

Other information that must be disclosed includes the sources of information in the file;[571] the names (and telephone numbers and addresses if requested) of the persons who have received such information in the preceding year (two years if it was for employment purposes);[572] the dates, original payees, and

566 15 USC s 1681h(a)(1).

567 15 USC s 1681g(a)(1). The FCRA initially only required that "the nature and substance" of the information should be revealed, and the consumer reporting agency was only requested to give a summary of the information in the file. Further, medical information in the file was not required to be disclosed. Note that this provision refers to "all" information in the consumer's file, not only information that has been entered into a consumer report (*Heath v Credit Bureau of Sheridan, Inc* 618 F 2d 693 (CA Wyo 1980)).

568 15 USC s 1681h(a)(2). Other forms of disclosure include disclosure to the consumer in person, by telephone, by electronic means, or by any other reasonable means (15 USC s 1681h(b)).

569 15 USC S 1681h(c).

570 15 USC S 1681h(d). Such person must provide reasonable identification. The consumer reporting agency may require the consumer to furnish a written statement granting permission to the consumer reporting agency to discuss the consumer's file in such person's presence.

571 The source of a purely investigatory report is excepted from this provision (in other words the name of the gossiping neighbour need not be disclosed). However, once an action is brought under the FCRA, such sources are also available under appropriate discovery procedures (15 USC s 1681g(a)(2)).

572 15 USC s 1681g(a)(3)(A). Once more an exception is made where the end user is a government agency or department that procures the report for purposes of determining the eligibility of the consumer to whom the report relates to receive access or continued access to classified information (15 USC s 1681g(3)(C)).

amounts of any checks upon which any adverse characterisation of the consumer is based;[573] a record of all inquiries received by the agency during the one-year period preceding the request that identified the consumer in connection with a credit or insurance transaction that was not initiated by the consumer.[574]

b Summary of rights

With each written disclosure by the agency to the consumer, a consumer reporting agency must also provide the consumer with a written summary of all the rights that the consumer has under the FCRA, and in the case of a consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, also a toll-free telephone number established by the agency, at which personnel are accessible to consumers during normal business hours.

The summary of rights must include:[575]

- ❒ a brief description of the FCRA and all the rights that it grants consumers
- ❒ an explanation of how consumers may exercise their rights
- ❒ a list of all federal agencies responsible for enforcing any provision of the Act
- ❒ a statement that the consumer may have additional rights under state law
- ❒ a statement that a consumer reporting agency is not required to remove accurate derogatory information from a consumer's file, unless the information is outdated or cannot be verified

4.3.2.8 Procedure in the event of disputed accuracy

a Reinvestigation of disputed information

573 15 USC s 1681g(a)(4).

574 15 USC s 1681g(a)(5). In certain circumstances, the FCRA allows consumer reporting agencies to make reasonable charges for disclosures. After an adverse notice has been given, no charge may be asked. For more detail, see 15 USC s 1681j and also see par 4.3.2.9.

575 15 USC s 1681g(c)(2).

The FCRA gives a consumer the opportunity to dispute the completeness or accuracy of any item of information contained in the consumer's file at a consumer reporting agency and to demand a reinvestigation.[576] The agency must investigate free of charge and record the current status of the disputed information or delete the item from the file within thirty days.[577] The furnishers of information must also receive prompt notice of the dispute. The notice must include all relevant information regarding the dispute that the agency has received from the consumer.[578]

Frivolous or irrelevant disputes may be terminated by a consumer reporting agency which has "reasonably determined" that the disputes are in fact frivolous or irrelevant.[579] The fact that the consumer has failed to provide sufficient information to allow the disputed information to be investigated also qualifies as a ground for termination.[580] When a consumer reporting agency has determined that a dispute is frivolous or irrelevant it must, within five days, notify the consumer of its determination.[581] Such a notice must include the reasons for the determination and identification of any information required to investigate the disputed information, which may consist of a standardised form describing the general nature of such information.[582]

When conducting a reinvestigation on disputed information in the file of a consumer, the consumer reporting agency must review and consider all relevant information submitted by the consumer with

576 15 USC s 1681i. Sherland 1984 *Wash LR* 401, 404 fn 25 argues that the term "reinvestigation", as far as consumer credit organisations are concerned, is a misnomer since these agencies do not initially investigate the information supplied to them. It is only when a consumer disputes the accuracy of information that they actually do their first investigation. A consumer investigating agency, on the other hand, is responsible for the initial investigation.

577 15 USC s 1681i(a)(1)(A). That period may be extended for 15 days in limited circumstances (15 USC ss 1681i(a)(1)(B) & (C)).

578 15 USC s 1681i(a)(2).

579 See eg *Williams v Colonial Bank* 826 F Supp 415 (MD Ala 1993).

580 15 USC s 1681i(a)(3)(A).

581 15 USC s 1681i(a)(3)(B).

582 15 USC s 1681i(a)(3)(C).

respect to the disputed information.[583] Information that is found to be inaccurate, incomplete or unverifiable must be promptly deleted from the consumer's file, or modified, as appropriate, on the basis of the results of the reinvestigation.[584] A consumer reporting agency must maintain reasonable procedures designed to prevent the reappearance of deleted information in a consumer's file and in consumer reports on the consumer.[585]

If any information has been deleted from a consumer's file the information may not afterwards be reinserted in the file, unless the person who furnishes the information certifies that the information is complete and accurate.[586] If previously deleted material is reinserted, the consumer reporting agency must notify the consumer of this within five days.[587] The notice must include a statement that the disputed information has been reinserted; the particulars of the furnisher of information that contacted the consumer reporting agency in connection with the reinsertion of such information; and a notice that the consumer has the right to add a statement to his or her file disputing the accuracy or completeness of the disputed information.[588]

Consumer reporting agencies that compile and maintain files on consumers on a nationwide basis must implement an automated system through which furnishers of information may report the results of an investigation that finds incomplete or inaccurate information in a consumer's file to other consumer

583 15 USC s 1681i(a)(4). A credit reporting agency that has been notified of potentially inaccurate information in a consumer's report may be required, in certain circumstances, to verify the accuracy of its initial source of information. Whether the agency has a duty to go beyond the original source depends on whether the consumer has alerted the agency of the possibility that the source may be unreliable, or whether the agency itself knows or should have known that the source is unreliable, and it also depends on the cost of verifying the accuracy of the source versus the possible harm the inaccurate reported information may cause the consumer (*Henson v CSC Credit Servs* 29 F 3d 280 (CA Ind 1994)).

584 15 USC s 1681i(a)(5)(A). *Pinner v Schmidt* 805 F 2d 1258 (CA La 1986).

585 15 USC s 1681i(a)(5)(C).

586 15 USC s 1681i(a)(5)(B)(i).

587 15 USC s 1681i(a)(5)(B)(ii).

588 15 USC s 1681i(a)(5)(B)(iii).

reporting agencies.[589]

The results of an investigation must be made known by the consumer reporting agency to the consumer within five days.[590] Such notice must include, in writing, the following infomation:[591]

- a statement that the reinvestigation has been completed

- a consumer report that is based upon the consumer's file after that file has been revised as a result of the reinvestigation

- a notice that, if requested by the consumer, a description of the procedure used to determine the accuracy and completeness of the information will be provided, including the business name and address of any furnisher of information contacted in connection with such information and the telephone number of such furnisher, if reasonably available

- a notice that the consumer has the right to add a statement to the consumer's file disputing the accuracy or completeness of the information[592]

- a notice that the consumer has the right to request that the consumer reporting agency furnish a notification of deleted or disputed information to any person designated by the consumer who has recieved a consumer report for employment purposes during the preceding two years, or within six months prior thereto for any other purpose[593]

589 15 USC s 1681i(a)(5)(D).

590 15 USC s 1681i(a)(6)(A).

591 15 USC s 1681i(a)(6)(B).

592 See par 4.3.2.8.b hereunder.

593 See par 4.3.2.8.b hereunder.

b Statement of dispute

If the reinvestigation does not resolve the dispute, the consumer may file a brief statement explaining the nature of the dispute.[594] In all subsequent disclosures, unless there are reasonable grounds to believe that the dispute is frivolous or irrelevant, the agency must clearly note that certain information has been disputed by the consumer and provide either the consumer's statement or a clear and accurate codification or summary thereof.[595] The agency must at the request of the consumer notify any specifically designated person who has received information on the consumer in the preceding six months (two years if it was for employment purposes) that such information has been deleted or is the subject of a dispute.[596]

4.3.2.9 Requirements regarding users of consumer reports

a Duties of users taking adverse action on the basis of information contained in consumer reports

A person who takes any adverse action[597] with respect to a consumer based on information contained in a consumer report must notify the consumer of such action,[598] and inform the consumer of the name, address and telephone number of the consumer reporting agency that furnished the report to the

594 15 USC s 1681i(b).The consumer reporting agency may limit such statements to not more than one hundred words if it assists the consumer to write a clear summary of the dispute.

595 15 USC s 1681i(c).The agency's duty to include a consumer's statement of dispute in a report only arises once the statement has been filed (*Mirocha v TRW, Inc* 805 F Supp 663 (SD Ind 1992)). Also see *Alexander v Moore & Associates. Inc* 553 F Supp 948 (DC Hawaii 1982).

596 15 USC s 1681i(d).

597 "Adverse decision" is extensively defined in 15 USC s 1681a(k), but basically means any unfavourable decision (such as a denial of, or increase in the charge for) insurance, employment, or a license.

598 15 USC s 1681m(a)(1). The notification may be made orally, in writing or electronically. See *Fischl v General Motors Acceptance Corp* 708 F 2d 143 (CA La 1983).

person.[599] The notification must make it clear to the consumer that the consumer reporting agency did not make the decision to take the adverse action and is unable to furnish to the consumer the specific reasons why the adverse action was taken.[600]

The person making the adverse decision must notify the consumer of his or her rights under the FCRA,[601] specifically the right to obtain a free copy of a consumer report on the consumer from the consumer reporting agency involved[602] and the right to dispute with a consumer reporting agency the accuracy or completeness of any information in a consumer report furnished by the agency.[603]

b Duties of users taking adverse action on basis of information obtained from third parties

Should a person deny a consumer credit for personal, family or household purposes, or increase the charge for such credit because of information (bearing upon the consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living) obtained from a person other than a consumer reporting agency, the user of such information must, when the consumer is informed about the adverse decision, also inform the consumer that he or she has the right to request reasons for such a decision. Upon receiving the request, the person must disclose the nature of the information to the consumer.[604]

---

599 15 USC s 1681m(a)(2)(A). Where a plaintiff is denied credit by a company, the company has to properly identify the credit reporting agency in the letter to the plaintiff. Failure to do so amounts to wilful noncompliance with the requirements of this section (*Carroll v Exxon Co USA* 434 F Supp 557 (DC La)).

600 15 USC s 1681m(a)(2)(B).

601 15 USC s 1681m(a)(3).

602 See par 4.3.2.7 as well as fn 574.

603 See par 4.3.2.8.

604 15 USC s 1681m(b)(1). Persons taking decisions based on information provided by affiliated companies also have similar duties. See 15 USC s 1681m(b)(2).

c Duties of users making credit or insurance solicitations on basis of information contained in consumer files

A person who uses a consumer report to solicit a credit or insurance transaction must with each solicitation make a clear and conspicuous statement that information contained in the consumer's consumer report was used in connection with the transaction. The statement must include a statement that the consumer received the offer of credit or insurance because he or she satisfied the criteria for creditworthiness or insurability under which the consumer was selected for the offer, but that the credit or insurance may not be extended if, after the consumer has responded to the offer, the consumer does not meet the selection criteria for the offer. The statement must also explain that the consumer has a right to prohibit information contained in his or her file at a consumer reporting agency from being used in connection with any credit or insurance transaction that is not initiated by the consumer, and the statement must explain how the consumer may exercise this right.[605]

d Limitation of liability

Liability for a violation of these provisions is excluded where a person can show by a preponderance of the evidence that at the time of the alleged violation reasonable procedures were maintained to ensure compliance with the provisions of the section.[606]

4.3.2.10 Responsibilities of furnishers of information to consumer reporting agencies

A person who regularly and in the ordinary course of business furnishes information to consumer reporting agencies has a duty to provide accurate information.[607] This duty comprises five aspects:

605 See par 4.3.2.3.d. The notification must include the address and telephone number of the notification system (15 USC s 1681m(d)(2)).

606 15 USC s 1681m(c).

607 The FCRA does not impose strict liability and a consumer reporting agency can escape liability if it (continued...)

❒ A prohibition on the reporting of inaccurate information

This refers specifically to the reporting of information which the person knows is inaccurate, or the reporting of information after the person has received notice from the consumer that it is inaccurate and it has been confirmed that the information contains errors.[608]

❒ A duty to correct and update information

A person who has furnished information which that person later determines to be incomplete or inaccurate has a responsibility to promptly notify the consumer reporting agency of this fact and to supply to the agency any corrections or additional information that may be necessary to make the information complete and accurate[609]

❒ A duty to provide the consumer reporting agency with a notice that the completeness or accuracy of the information has been disputed by the consumer, if that is the case

❒ A duty to notify the consumer reporting agency of a closed credit account

A person who furnishes information to a consumer reporting agency regarding a consumer who has a credit account with that person has a duty to notify the agency of the voluntary closure of the account by the consumer, as part of information regularly furnished for the period in

607(...continued)
establishes that an inaccurate report was generated despite the fact that the agency followed reasonable procedures (*Guimond v Trans Union Credit Info Co* 45 F 3d 1329 (CA Cal 1995)).

608 15 USC s 1681s–2(a)(1). This section is subject to administrative enforcement under 15 USC s 1681s by the federal and state agencies and officials identified in that section (see 15 USC s 1681s–2(d)). (On s 1681s, see par 4.3.2.13.) Civil liability is excluded from this section, but the state may bring an action on behalf of consumers in terms of 15 USC s 1681s(c)(1)(B) (see 15 USC s 1681s–2(c)).

609 15 USC s 1681s–2(a)(2).

which the account was closed.[610]

❒ A duty to provide notice of delinquency of accounts

A person who furnishes information to a consumer reporting agency regarding a delinquent account being placed for collection, charged to profit or loss, or subjected to any similar action has a duty to notify the agency, within 90 days, of the month and year of the commencement of the delinquency.[611]

4.3.2.11 Duties of furnishers of information upon notice of dispute

After receiving notice of a dispute with regard to the completeness or accuracy of information provided by a person to a consumer reporting agency, the person is obliged to conduct an investigation with respect to the disputed information, to review all relevant information provided by the consumer reporting agency, to report the results of the investigation to the consumer reporting agency and to all other consumer reporting agencies to which the person furnished the information if the information should be found to be incomplete or inaccurate.[612]

4.3.2.12 Remedies and penalties

a Civil remedies

A consumer may begin an action in a district court or in any other court of competent jurisdiction within

610 15 USC s 1681s–2(a)(4).

611 15 USC s 1681s–2(a)(5).

612 15 USC s 1681s–2(b)(1).

two years[613] against an agency or user who wilfully,[614] knowingly or negligently fails to comply with any requirement of the Act.

In the case of wilful noncompliance, a person is liable to the consumer for actual damages sustained by the consumer as a result of the failure or damages of not less than $100 and not more than $1,000, or in the case of liability of a natural person for obtaining a consumer report under false pretences or knowingly without a permissible purpose, actual damages sustained by the consumer as a result of the failure or $1,000, whichever is the greater.[615] The court may also award punitive damages[616] and the costs of the action together with reasonable attorney's fees .[617]

Any person who obtains a consumer report from a consumer reporting agency under false pretenses or knowingly without a permissible purpose, is liable to the consumer reporting agency for actual damages sustained by the consumer reporting agency or $1,000, whichever is greater.[618]

A person who was negligent in failing to comply with a requirement imposed by the FCRA with respect to a consumer is liable to that consumer for actual damages sustained and the costs of the action together with reasonable attorney's fees as determined by the court.[619]

A court must award to the prevailing party attorney's fees reasonable in relation to the work expended,

613 15 USC s 1681p.

614 To establish that the defendant acted with wilful noncompliance, it must be shown that the defendant has knowingly and intentionally committed the act in conscious disregard for the rights of others (*Stevenson v TRW, Inc* 987 F 2d 288 (CA Tex 1993)).

615 15 USC s 1681n(a)(1). According to *Thompson v San Antonio Retail Merchants Asso* 682 F 2d 509 (CA Tex 1982), humiliation and mental distress form part of the damage that can be recovered, even where there are no out-of-pocket (ie patrimonial) expenses.

616 15 USC s 1681n(a)(2).

617 15 USC s 1681n(a)(3).

618 15 USC s 1681n(b).

619 It is not a predicate for liability under the FCRA that the consumer must have been denied credit (*Guimond v Trans Union Credit Info Co* 45 F 3d 1329 (CA Cal 1995)).

if the court find that an unsuccessful pleading, motion or other paper filed in connection with a civil action for noncompliance with the provisions of the FCRA, was filed in bad faith or for purposes of harassment.[620]

b Limitation of liability

Prior to the enactment of the FCRA, state common law treated the injury that resulted from an unfair credit report as defamation. The FCRA supplanted the state law of defamation in this area, and substituted a statutory action for the common law action.[621] The FCRA specifically provides that a consumer may not bring an action in the nature of defamation, an invasion of privacy, or negligence, other than the actions discussed in the preceding paragraph, based on information disclosed to the consumer, except if such information is false and was furnished with malice or wilful intent to injure the consumer.[622]

c Criminal penalties

An officer or employee of the agency who knowingly and wilfully gives out information to a person not authorised to receive that information, may be fined[623] or imprisoned for not more than two years, or both.[624] The same penalties are applicable to a person who obtains information under false pretences.[625]

4.3.2.13 Administrative enforcement

620 15 USC s 1681n(c) & s 1681o(b).

621 See Blair & Maurer 1984 *Mo LR* 289, 291.

622 15 USC s 1681h(e). See *Thornton v Equifax, Inc* 619 F 2d 700 (CA Ark 1980);*Mitchell v Surety Acceptance Corp* 838 F Supp 497 (DC Colo 1993).

623 In terms of 18 USC.

624 15 USC s 1681r.

625 15 USC s 1681q. Where a merchant obtained a credit report from a local credit bureau on a political candidate for purposes of investigating improper campaign financing procedures, the credit information was obtained under false pretenses (*Hansen v Morgan* 582 F 2d 1214 (CA Idaho 1978)).

Administrative enforcement of the FCRA is entrusted to the Federal Trade Commission (FTC), who can enforce the FCRA in terms of its powers under the Federal Trade Commission Act.[626]

Two important new provisions have been introduced in recent amendments of the FCRA. First of all, the FTC may commence a civil action to recover a civil penalty in a district court against any person who violates the FCRA, where such violation is knowingly committed and "constitutes a pattern or practice of violations". In such action, the person will be liable for a civil penalty of not more than $2,500 per violation.[627]

Secondly, a state may bring an action to enjoin violations of the FCRA,[628] and may also bring an action on behalf of the residents of the state to recover damages as a result of the violations.[629]

4.3.2.14 Disclosures to FBI

The FCRA also contains a provision enabling the Federal Bureau of Investigation (FBI) to obtain information from consumer reporting agencies for counterintelligence purposes. A consumer reporting agency is obliged to furnish to the FBI the names and addresses of all financial institutions at which a consumer maintains an account, to the extent that such information is available in the files of the agency, when presented with a written request for that information, signed by the Director of the FBI, which certifies compliance with FCRA.

---

626 15 USC s 1681s(a), referred to as FTCA. A violation of any requirement or prohibition of the FCRA constitutes an "unfair or deceptive act or practice in commerce" as prohibited by the FTCA, irrespective of whether that person is engaged in commerce or meets any jurisdictional tests in the FTCA (15 USC s 1681s(a)(1). For other agencies that may be involved, see 15 USC s 1681s(b).

627 15 USC s 1681s(a)(2).

628 Consumers cannot enjoin credit reporting agencies (*Mangio v Equifax, Inc* 887 F Supp 283 (SD Fla 1995)).

629 15 USC s 1681s(c). Eg, the states of Texas, California, Michigan, Alabama and Idaho brought suit in 1991 against a major credit information company (Thompson Ramo Wooldridge (TRW)) for the selling of private consumer data to direct marketing firms without the consent of the data subjects and for the failure of TRW to correct erroneous credit histories of consumers (Madsen *Personal data protection* 134). According to Madsen these suits represent a major development in personal data protection in the USA.

The Director may make such a certification only if the Director has determined in writing that such information is necessary for the conduct of an authorised foreign counterintelligence investigation, and that there are specific and articulable facts giving reason to believe that the consumer is a foreign power or an official of a foreign power; or is an agent of a foreign power and is engaging in an act of international terrorism or clandestine intelligence activities that may involve a violation of the criminal statutes of the United States.[630]

A consumer reporting agency must also furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the FBI when presented with a written request, signed by the Director. In this instance the Director must determine in writing that the information is necessary for the conduct of an authorised counterintelligence investigation and that there is information giving reason to believe that the consumer has been in contact with a foreign power or an agent of a foreign power.[631]

4.3.2.15 Disclosures to government agencies for counterterrorism purposes

After 11 September 2001, the FCRA was amended to allow the disclosure of information in a consumer's file to a government agency authorised to conduct investigations or intelligence activities related to international terrorism.[632]

4.3.3 Summary

The purpose of the FCRA is to balance the need of the credit, insurance and employment industries for fair and accurate information on consumers against the right of consumers that the confidentiality, accuracy and relevance of such personal information be ensured. The Act consequently imposes a duty on consumer reporting agencies, which have assumed the responsibility for collecting and evaluating

630 15 USC s 1681u(a).

631 15 USC s 1681u(b).

632 15 USC s 1681v, inserted by Pub L 107–56 (26 October 2001).

consumer credit, to adopt reasonable procedures to meet the needs of commerce and at the same time exercise their functions with fairness, impartiality and a respect for the consumer's right to privacy. In terms of this Act a consumer may *inter alia* find out what is in his or her file at a credit bureau, dispute the accuracy of information in the file, demand an investigation into the correctness of disputed information, demand the deletion of obsolete and inaccurate information and elect to be removed from lists for unsolicited credit and insurance offers. Access to the consumer's file is limited to parties with a purpose recognised by the FCRA. A consumer must be informed if information in his or her file has been used to his or her detriment. A consumer's consent is required for reports that are provided to employers or for reports that contain medical information. A consumer may seek damages from persons who do not comply with the FCRA. The FTC may also enforce the FCRA.

5 DATA PROTECTION IN USA AND "SAFE HARBOR" AGREEMENT

In brief, the current position in the United States is as follows: The right to privacy is recognised both in tort law and in constitutional law. However, because tort law and constitutional law protection have proved to be ineffective in dealing with the dangers of information technology, legislation has become the most important tool in protecting personal information involved in data processing. The United States does not have a general data protection law at federal level; instead different pieces of legislation are involved. This means that different levels of protection are accorded to personal information, depending on the type of personal information involved. Protection of personal information in the private sector especially is still too limited. The United States also needs an independent data protection authority.[633]

The question arose whether the Unites States would be deemed to have "adequate" data protection in the sense in which the term is used in the European Union's data protection directive of 1995.[634] Article 25 of the Directive prohibits the transfer of personal data from EU countries to third countries that do not provide adequate data protection. This provision (in its final and draft forms) has raised fears

633 See Flaherty *Surveillance societies* 367.

634 See ch 3 par 4.2.7.

in the US that the free flow of data between the US and Europe will be hampered.[635]

Two American law professors undertook a study of US data protection law for the Commission of the European Communities. In their report, published in book form in 1996, they concluded that it is impossible to say in general that data protection in the US is "sufficient", but that the answer depends on the contexts in which personal data are processed.[636]

EPIC[637] reports that the USA strongly lobbied[638] the EU member countries to find the US system adequate and in 1998 the USA and the EU began negotiating a "Safe Harbor" agreement in order to ensure the free flow of personal information to the US.[639] The "Safe Harbor" agreement consists of a set of privacy principles agreed upon by the US Department of Commerce and the Internal Market Directorate of the European Commission. The principles require the organisations who choose to sign it to provide individuals with a "clear and conspicuous" notice of the type of information they collect, the purposes for which the information may be used and the names of third parties to whom it may be disclosed. This notice must be given at the time of the collection of any personal information or as soon

635 See Gellman 1996 *Villanova LR* 129; Berkvens 1995 *Computer L & Prac* 38; Schwartz 1995 *Iowa LR* 471; 1991 (Nov /Dec) *TDR* 8; Trubow 1992 *NW J Int L & Bus* 159; Cole 1985 *NYUJ Int L & Pol* 893; Rosenbaum 1992 *Jurimetrics JL* 1 8.

636 Schwartz & Reidenberg *Data privacy law* 205 381. Their conclusions were that American law in the public sector possesses the general means for data protection, but that it does not completely and successfully carry out such data protection (206). The US private sector, they concluded, does not uniformly fulfil the complete set of basic elements found in the European principles of fair information practice (387). As Simitis puts it in the introduction to this book, in the USA "[t]he answers to the 'adequacy' question is as variable as the contexts in which personal data are processed" (Schwartz & Reidenberg *Data privacy law* x).

637 EPIC *Privacy and human rights* 17.

638 For a discussion of the lobbying strategies and tactics of American businesses, see Regan "American business and the data protection directive".

639 In 1999 the Working Party established by a 29 of the EU Directive (see ch 3 par 4.2.8.3) found that "the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot ... be relied upon to provide adequate protection in all cases for personal data transfers from the European Union" (Data Protection Working Party *Opinion 1/99 concerning the level of data protection in the united states* 2).

thereafter as is practicable. Where sensitive information[640] is collected, the individual must give express consent to the collection. Organisations wanting to transfer data to a third party may do so only if the third party subscribes to the "Safe Harbor" principles, or signs an agreement to protect the data.

The idea was that companies in the US would voluntarily self-certify to adhere to these principles. The companies would then be presumed to provide adequate privacy protection and could continue to receive personal information from the EU. The agreement was approved in 2000, but the Commission promised to re-open negotiations if the remedies open to its citizens proved to be inadequate.[641]

EPIC[642] reports that both privacy advocates and consumer groups in the United States were critical of the European Commission's decision to approve the agreement. The report points to the following negative aspects of this agreement:

> The agreement rests on a self-regulatory system whereby companies merely promise not to violate their declared privacy practices. There is little enforcement or systematic review of compliance. The Safe Harbor status is granted at the time of self-certification. There is no individual right to appeal or right to compensation for privacy infringements. There is an open-ended grace period for United States signatory companies to implement the principles. The agreement will only apply to companies overseen by the Federal Trade Commission and Department of Transportation (excluding the financial and telecommunications sectors) and there are special exceptions granted for public records information protected by European Union law.

In July 2002 the Data Protection Working Party established by article 29 of the European Union

640 Eg, information relating to race, religious beliefs and criminal records.

641 For more information on the Safe Harbor agreement, see EPIC *Privacy and human rights* 16 *et seq*; Clear 2002 *J Mar J Computer & Inf L* 981; Ewing 2002 *Houston J Int L* 315; Bull 2001 *Computer L & Sec Rep* 239; Blanke 2000 *Alb LJ Sci & Tech* 57.

642 EPIC *Privacy and human rights* 18.

Directive on data protection[643] issued a working paper on the functioning of the "Safe Harbor" agreement.[644] The Working Party expressed the intention to study the agreement in further detail with particular regard to possible gaps between the principles and the implementing practices, as well as the transparency requirements to be met by the organisations. The Commission plans to issue a full evaluation of the agreement during 2003.

643 See ch 3 par 4.2.8.3.

644 Data Protection Working Party *Working document on the functioning of the Safe Harbor Agreement* 3.